NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

AC/323(IST-067)TP/317

www.rto.nato.int

RTO TECHNICAL REPORT **TR-IST-067**

Technical Communications in Urban Operations

(Les communications techniques en opérations urbaines)

This Report documents the Findings of Task Group IST-067.

Published September 2010

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

AC/323(IST-067)TP/317

www.rto.nato.int

RTO TECHNICAL REPORT **TR-IST-067**

Technical Communications in Urban Operations

(Les communications techniques en opérations urbaines)

This Report documents the Findings of Task Group IST-067.

The Research and Technology Organisation (RTO) of NATO

RTO is the single focus in NATO for Defence Research and Technology activities. Its mission is to conduct and promote co-operative research and information exchange. The objective is to support the development and effective use of national defence research and technology and to meet the military needs of the Alliance, to maintain a technological lead, and to provide advice to NATO and national decision makers. The RTO performs its mission with the support of an extensive network of national experts. It also ensures effective co-ordination with other NATO bodies involved in R&T activities.

RTO reports both to the Military Committee of NATO and to the Conference of National Armament Directors. It comprises a Research and Technology Board (RTB) as the highest level of national representation and the Research and Technology Agency (RTA), a dedicated staff with its headquarters in Neuilly, near Paris, France. In order to facilitate contacts with the military users and other NATO activities, a small part of the RTA staff is located in NATO Headquarters in Brussels. The Brussels staff also co-ordinates RTO's co-operation with nations in Middle and Eastern Europe, to which RTO attaches particular importance especially as working together in the field of research is one of the more promising areas of co-operation.

The total spectrum of R&T activities is covered by the following 7 bodies:

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These bodies are made up of national representatives as well as generally recognised 'world class' scientists. They also provide a communication link to military users and other NATO bodies. RTO's scientific and technological work is carried out by Technical Teams, created for specific activities and with a specific duration. Such Technical Teams can organise workshops, symposia, field trials, lecture series and training courses. An important function of these Technical Teams is to ensure the continuity of the expert networks.

RTO builds upon earlier co-operation in defence research and technology as set-up under the Advisory Group for Aerospace Research and Development (AGARD) and the Defence Research Group (DRG). AGARD and the DRG share common roots in that they were both established at the initiative of Dr Theodore von Kármán, a leading aerospace scientist, who early on recognised the importance of scientific support for the Allied Armed Forces. RTO is capitalising on these common roots in order to provide the Alliance and the NATO nations with a strong scientific and technological basis that will guarantee a solid base for the future.

Published September 2010

ISBN 978-92-837-0111-8

Table of Contents

List of Figures/Tables

List of Acronyms

A/G/A	Air-to-Ground-to-Air
ADAMS	Allied Deployment And Movement System
ADC	Analog-to-Digital Converter
AJ	Anti-Jamming
API	Application Programming Interface
BDE	Brigade
BFT	Blue Forces Tracking
BLOS	Beyond Line Of Sight
BS	Base Station
C2	Command and Control
C3	Command, Control and Communications
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CCEB	Communications and Electronics Board
CIMIC	Civil-Military Co-operation
CIR	Critical Information Requirement
CIS	Communication and Information Systems
CMRS	Commercial Mobile Radio Services
CNR	Combat Net Radio
COMSEC	Communications Security
CONOPS	Concept of Operations
COP	Common Operations Picture
COTS	Commercial-Off-The-Shelf
CPE	Consumer Premise Equipment
CR	Cognitive Radio
CS	Core Service
CSS	Combat Support Service
DAC	Digital-to-Analog Converter
DFB	Dynamic Frequence Broker
EPM	Electronic Protective Measures
EW	Electronic Warfare
FMSC	Frequency Management Subcommittee
FPGA	Field Programmable Gate Array
FS	Functional Service
GPS	Global Positioning System
HCDR	High Capacity Data Radio
HF	High Frequency (3 – 30 MHz)
HQ	Headquarters
HUMINT	Human Intelligence
ICC	Integrated Command and Control
ICT	Information and Communications Technology
IED	Improvised Electronic Devices

IEEE	Institute of Electrical and Electronics Engineers
IER	Information Exchange Requirements
IETF	European Telecommunications Standards Institute
IMINT	Imagery Intelligence
IP	Internet Protocol
IST	Information Systems Technology
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
ITU	International Telecommunication Union
IW	Information Warfare
JCOP	Joint Common Operating Picture
LAN	Local Area Network
LC2IS	Land Command and Control Information Services
LOCE	Linked Operational Intelligence Centers Europe
LOGFAS	Logistic Functional Area Services
LOS	Line Of Sight
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
LTE	Long Term Evolution
MAC	Medium Access Control
MANET	Mobile Ad-Hoc Network
MIMO	Multiple-Input Multiple-Output
MIPS	Million Instructions Per Second
MoE	Measures of Effect
MOOTW	Military Operations Other Than War
MOUT	Military Operations in Urban Terrain
MS	Mission Secret
MUOS	Mobile User Objective System
NC3A	NATO C3 Agency
NCO	Network Centric Operations
NCW	Network Centric Warfare
NEC	Network Enabled Capability
NGO	Non-Governmental Organization
NM	Network Management
NRF	NATO Reaction Force
NS	NATO Secret
NU	NATO Unclassified
NVIS	Near Vertical Incidence Sky-Wave
OPLAN	Operation Plan
PLMRS	Private Land Mobile Radio Services
PMR	Private Mobile Radio
QoS	Quality of Service
RF	Radio Frequency
RTG	Research Task Group
SA	Situational Awareness
SATCOM	Satellite Communications

SDR	Software Defined Radio
SHF	Super High Frequency (3 – 30 GHz)
SIGINT	Signals Intelligence
SIMO	Single-Input Multiple-Output
SM	Spectrum Management
SMS	Short Message Service
STF	Spectrum Task Force
TAP	Technical Activity Proposal
TCS	Tactical Communication Systems
TDMA	Time Division Multiple Access
TETRA	Terrestrial Trunked Radio
TOR	Terms Of Reference
TRANSEC	Transmission Security
TTP	Tactics, Techniques, & Procedures
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency (300 MHz – 3 GHz)
UO	Urban Operations
USECT	Understand, Shape, Engage, Consolidate & Transition
VHF	Very High Frequency (30 – 300 MHz)
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WRAN	Wireless Regional Area Network
WRC	World Radiocommunication Conference

IST-067 Programme Committee

CANADA

Dr. Philip VIGNERON
Communications Research Centre Canada
3701 Carling Avenue, P.O. Box 11490, Stn. H
Ottawa, Ontario K2H 8S2
Email: philip.vigneron@crc.ca

GERMANY

Dr. Markus ANTWEILER
FGAN/FKIE
Neuenahrer Strasse, 20, D-53343 Wachtberg
Email: markus.antweiler@fkie.fraunhofer.de

Mr. Thomas BACHRAN
FGAN/FOM
Neuenahrer Strasse, 20, D-53343 Wachtberg
Email: bachran@fgan.de

Prof. Jürgen GROSCHE
FGAN/FKIE Director
Neuenahrer Strasse, 20, D-53343 Wachtberg
Email: juergen.grosche@fkie.fraunhofer.de

ITALY

Mr. Mario DI STEFANO
SCUTI – Scuola Trasmissioni ed Informatica
dell'Esercito Italiano
Via dei Genieri, 287, 00143-Roma Cecchignola
Email: Mario.DiStefano@selex-comms.com

Lt. Fabrizio LAMBIASE
SCUTI – Scuola Trasmissioni ed Informatica
dell'Esercito Italiano
Via dei Genieri, 287, 00143 Roma Cecchignola
Email: casezsvilc4@sctrasm.esercito.difesa.it

NETHERLANDS

Mr. Ruud OVERDUIN
TNO
P.O. Box, 5050 Delft
Email: Ruud.Overduin@tno.nl

NORWAY

Prof. Torleiv MASENG
Director of Research
Norwegian Defence Research Establishment (FFI)
P.O. Box 25, NO-2027 Kjeller
Email: torleiv.maseng@ffi.no

Ms. Elin Sundby BOYSEN
Research Assistant
Norwegian Defence Research Establishment (FFI)
P.O. Box 25, NO-2027 Kjeller
Email: Elin-Sundby.Boysen@ffi.no

POLAND

Prof. Marek AMANOWICZ
Military Communication Institute
05-130 Zegrze
Email: m.amanowicz@wil.waw.pl

Dr. Rafal PIOTROWSKI
Military Communication Institute
05-130 Zegrze
Email: r.piotrowski@wil.waw.pl

UNITED KINGDOM

Prof. Bob MADAHAR
Dstl, Information Management Dept.
Bldg. 5, Room G02/438
Porton, Salisbury, Wilts SP4 0JQ
Email: bkmadahar@dstl.gov.uk

Mr. William GORST
Dstl, Information Management Dept.
Bldg. 5, Room G02/438
Porton, Salisbury, Wilts SP4 0JQ
Email: WDGORST@dstl.gov.uk

UNITED STATES

Dr. Michael BOWMAN (Chair)
Murray State University
Center for Telecommunications Systems
Management
207 Industry and Technology Murray
KY 42071-3347
Email: michael.bowman@murraystate.edu

Dr. James GANTT
Murray State University
Center for Telecommunications Systems
Management
207 Industry and Technology Murray
KY 42071-3347
Email: james.gantt@murraystate.edu

Technical Communications in Urban Operations

(RTO-TR-IST-067)

Executive Summary

Communication in and between the multiple dimensions of urban environments is an extremely difficult technology challenge. Urban structures, materials, object densities and configurations (such as urban canyons), interference from a large diversity of electronic devices and power constraints associated with man-portable radios significantly degrade wireless communications.

The purpose of this Task Group was to investigate and suggest ways to improve tactical wireless RF communications in a wide spectrum of urban operations. There are lessons in this report for military personnel on the complexities of communicating in urban environments and which technologies may solve some of their tactical communications issues. There are lessons for the industry and research communities that should help them understand the tactical-urban environment so that they can better focus their research and experimentation.

Increasingly, NATO nations are involved in traditional and non-traditional military operations in towns and cities occupied by a combination of non-combatants and hostile forces. Of all the missions faced by NATO, these combat and stability operations are the most challenging. This three-dimensional battlefield, both above and below ground, places significant and severe stress on today's communications systems. Increasing dependence on information exchange at all levels is driving the demand for greater communication availability and throughput for military operations. Dependency on communications, especially at battalion level and below, is maximized in urban environments to compensate for loss of visual contact between small teams and to their parent organizations as they disappear into alleys, multi-story buildings, and subterranean systems (sewer systems and tunnels). While communications dependency is rising, its performance in urban settings suffers from radio frequency (RF) transmission range reductions caused by line-of-sight issues and attenuation due to buildings, structures and terrain; as well as interference from other local electromagnetic systems. In the case of peacekeeping missions, peace enforcement, or disaster relief, cooperation with existing civil authorities and interoperability with civil communications infrastructure will be essential. All of this should drive the development of new concepts of operations, requiring new tactical communication systems or novel ways of deploying or using existing tactical communication systems in urban operational environments.

Technology advances such as SDR, Cognitive Radio, MANET, MIMO, WiMAX, and Dynamic Spectrum Allocation have the potential to improve tactical communications in urban environments, and while proper tactics, techniques, and procedures based on lessons learned from on-going urban operations can significantly improve communications in these environments, the bottom line is that current technology and systems are NOT adequate to support fully integrated NCW operations in urban environments.

None of the approaches discussed in this report are a "one size fits all" solution for tactical communications in urban environments. Each approach has strengths and weaknesses. It will require the synergistic combination of the results from several of these approaches to fully allow the implementation of NATO NEC in urban operations. Future systems must be able to adapt rapidly to the unpredictable complex urban environment as much as possible and as autonomously as possible. This implies constant compromises by autonomously selecting the proper modes of operation. This report describes some enabling technologies that in time may solve these communications issues.

Les communications techniques en opérations urbaines

(RTO-TR-IST-067)

Synthèse

La communication à l'intérieur des volumes et entre les volumes multiples de l'environnement urbain, est un défi technologique extrêmement difficile. Les structures urbaines, les matériaux, la configuration et la densité des éléments (comme les canyons urbains), l'interférence d'une grande diversité de dispositifs électroniques et les contraintes de puissance associées aux radios portables dégradent sensiblement les communications sans fil.

L'objet de ce groupe de travail était de rechercher et de proposer des moyens pour améliorer les communications tactiques RF sans fil dans un large spectre d'opérations urbaines. Ce rapport apporte des enseignements au personnel militaire sur la complexité de communiquer en milieu urbain et indique les technologies qui peuvent résoudre quelques problèmes de communications tactiques. Il apporte des enseignements aux communautés de l'industrie et de la recherche, qui devraient les aider à comprendre l'environnement urbain tactique afin qu'elle puisse mieux orienter leurs recherches et expérimentations.

Les nations de l'OTAN sont de plus en plus impliquées dans des opérations militaires conventionnelles et non conventionnelles dans des villes et des cités occupées par un mélange de non combattants et de forces hostiles. De toutes les missions de l'OTAN, ces opérations de combat et de stabilisation sont les plus délicates. Ce champ de bataille tridimensionnel, à la fois au-dessus et en-dessous du sol, impose une pression significative très intense sur les systèmes de communications actuels. La dépendance croissante à l'échange des informations à tous les niveaux oriente la demande pour une disponibilité et un débit des communications plus importants pour les opérations militaires. La dépendance vis-à-vis des communications, en particulier au niveau bataillon et en-dessous, est maximisée en milieu urbain pour compenser la perte de contact visuel entre les petites équipes et avec leurs organismes d'appartenance quand ils disparaissent dans des allées, des immeubles à plusieurs étages et des souterrains (égouts et tunnels). Alors que la dépendance augmente, les performances des communications en milieu urbain souffrent d'une réduction de la gamme de transmissions radio RF provoquée par des problèmes de portée visuelle et d'atténuation due aux immeubles, aux structures et au terrain aussi bien qu'aux interférences avec les systèmes électromagnétiques locaux. Dans le cas des missions de maintien de la paix, de renforcement de la paix ou d'opérations de secours, la coopération avec les autorités civiles existantes et l'interopérabilité avec l'infrastructure civile des communications est essentielle. Tout ceci doit impliquer le développement de nouveaux concepts d'opérations, requérant des systèmes de communication tactiques nouveaux ou de nouveaux moyens de déploiement ou d'utilisation des systèmes de communication tactiques en milieu opérationnel urbain.

Les avancées technologiques comme le SDR, la Radio Cognitive, le MANET, le MIMO, le WiMAX, le Dynamic Spectrum Allocation peuvent potentiellement permettre d'améliorer les communications tactiques en milieu urbain. Alors que les tactiques, les techniques et les procédures basées sur les enseignements tirés des opérations urbaines en cours peuvent améliorer sensiblement les communications dans ces environnements, la réalité montre que la technologie et les systèmes actuels NE SONT PAS adaptés pour soutenir des opérations entièrement résaux centrés (NCW) en milieu urbain.

Aucune des approches débattues dans ce rapport ne donne une solution pour les communications tactiques en milieu urbain. Chaque approche a ses forces et ses faiblesses. Il va falloir recourir à l'application en

synergie des résultats de plusieurs de ces approches pour permettre l'implantation totale du NEC de l'OTAN en milieu urbain. Les systèmes futurs doivent s'adapter le plus rapidement possible et d'une manière la plus autonome possible à l'environnement urbain complexe et imprévisible. Ceci implique des compromis constants en sélectionnant les bons modes d'opérations de façon autonome. Ce rapport décrit quelques technologies susceptibles d'aider à résoudre en temps voulu ces problèmes de communication.

Chapter 1 – INTRODUCTION

1.1 BACKGROUND AND JUSTIFICATION

The purpose of this Task Group was to investigate and suggest ways to improve tactical wireless RF communications in a wide spectrum of urban operations. Increasingly, NATO nations are involved in traditional and non-traditional military operations in towns and cities occupied by a combination of non-combatants and hostile forces. Of all the missions faced by NATO, these combat and stability operations are the most challenging. This three-dimensional battlefield, both above and below ground, places significant and severe stress on today's communications systems.

Increasing dependence on information exchange at all levels is driving the demand for greater communication availability and throughput for military operations. Dependency on communications, especially at battalion level and below, is maximized in urban environments to compensate for loss of visual contact between small teams and to their parent organizations as they disappear into alleys, multi-storey buildings, and subterranean systems (sewer systems and tunnels). While communications dependency is rising, its performance in urban settings suffers from radio frequency (RF) transmission range reductions caused by line-of-sight issues and attenuation due to buildings, structures and terrain; as well as interference from other local electromagnetic systems. In the case of peacekeeping missions, peace enforcement, or disaster relief, cooperation with existing civil authorities and interoperability with civil communications infrastructure will be essential. All of this should drive the development of new concepts of operations, requiring new tactical communication systems or novel ways of deploying or using existing tactical communication systems in urban operational environments.

1.2 IST-067 OBJECTIVES

1) To understand urban military communications operational requirements, utilizing NATO subject matter experts and studies such as Land Operations 2020, Urban Operations 2020 (SAS-030), and various National studies.

2) To define technical challenges in meeting these urban operations communications requirements.

3) Determine the ability to meet these challenges with current communications systems and identify likely shortcomings.

4) To identify, assess, and report on collaborative trials and/or assessment activities that will lead to a greater understanding of the true communication capabilities, complementarities and limitations associated with military operations in urban environments.

5) Determine communication technology development requirements for current, near-term (2010), and far-term (2020) solutions.

1.3 TOPICS INVESTIGATED

1) Communication modalities appropriate to address the military tactical communications requirements identified in other ongoing or completed studies:

   a) Technical, operational, and organizational aspects of communications.

   b) Visions for near-term and future net-centric operations.

c) Seamless information exchange and interoperability among coalition nations / civil authorities and infrastructure. This requirement is driven by the NATO NEC and trend towards the formation of multi-national units at lower military levels.

2) Communication technologies that are current state-of-the-art, near-term capabilities, and far term capabilities:

   a) Technologies such as: narrow band, wide band (e.g. spread spectrum, Adaptive (mobile) MIMO), cognitive radio, high altitude platform relays, software definable and (SCA-based) software defined radios, MANET, and multiple access approaches.

   b) Standardization of communications capabilities / inter-working with host nation / commercial communications.

3) Related technical topics in consultation with other Panels or with invited subject matter experts:

   a) Power requirements.

   b) Size and weight constraints.

   c) Information exchange, protocols, bandwidth requirements, and exploitation.

4) Deployment, concepts of operations, and doctrine associated with tactical communications in urban environments, with an emphasis on lower level tactical operations at the company and below:

   a) Utilizing military users, workgroup members, and consultants, examined current concept of operations and doctrine with a focus on network centric operations.

   b) Examined how the urban environment can be used to enhance tactical communications. For example, tall buildings can be used as repeaters, electromagnetic dead space can be avoided, or electrical wiring in a building can be used as an antenna.

   c) Discussed how electromagnetic propagation can impact on the scheme of maneuver (e.g. devise avenues of attack that avoid radio dead spots).

   d) Discussed how communication has a more significant impact on the urban operations planning process.

1.4 RELATED TOPICS NOT INVESTIGATED

1) Information operations – both offensive and defensive.

2) Subterranean systems.

3) This report contains a system level discussion, not technical details like specific protocols, detailed security schemes, web services, or service oriented architecture.

1.5 DELIVERABLES AND END PRODUCT

1) This final report summarizing the Task Group's findings and activities.

2) IST-083/RSY-018 Symposium on *Military Communications with a Special Focus on Tactical Communications for Network Centric Operations* held in Prague, Czech Republic, 21 and 22 April 2008. The Symposium presentations fit into six related groupings: Software Defined Radio (SDR), Network and Resource Management, Performance, Urban Communications, Security, and Future Services in a Changing World. A mix of current, developing and future capabilities were presented to

address the increasingly complex operational environments faced by NATO forces. An important conclusion was that the land environment is the most challenging communications environment faced by NATO. Dependency on communications, especially at the lowest tactical levels, has increased to compensate for loss of visual contact between small teams and to their parent organizations as they disappear in alleys, multi-storey buildings, and subterranean tunnels. Increasing dependence on information exchange at all levels is driving the demand for greater communication availability and throughput. While communications dependency is rising, its performance suffers from radio frequency (RF) transmission range reductions caused by line-of-sight issues and attenuation due to buildings, structures and terrain; as well as interference from other local electromagnetic systems. All of this drives the development of new concepts of operations, requiring new tactical communication systems or novel ways of deploying or using existing tactical communication systems.

1.6 ASSUMPTIONS AND LIMITATIONS

IST-067 consisted primarily of twelve people from eight nations as listed above. Important assumptions that governed the operation, conduct, and results of the group included:

- Participation was voluntary.
- National participation, and participants from a given nation, could (and did) fluctuate.
- Assigned participants would (and did) have appropriate technical and military operational backgrounds and skills.
- Work group participants included military personnel, government employees, defence contractors, and academics.
- The work group could (and did) call upon technical support from their home nations and organizations as necessary.
- The work group had no direct control over any research and development funding.
- The work group did not attempt to influence the creation, direction, or results of research and development programs.
- A vast amount of communications system related research and development is currently being conducted by governments, industry, and academia and work group member assumed they would have adequate (but not complete) access to information on these efforts and would be free to share the information within the group.
- The work group could (and did to a limited extent) access and utilize national research program results, labs, project offices and personnel, and defence industry personnel and data.
- Given the assumptions listed here, and the significant limitations identified in the next section, the work group's primary purpose was sharing of information about the research, development and acquisition of tactical communications systems suitable for use in urban operations that is occurring in each of the participating nations. The expectation was that sharing this information would help eliminate redundant efforts among participants and improve the communications capability of each nation.

In addition to the assumptions listed above that proved to be true, the important limitations listed below constrained what could (and was) accomplished by the work group:

- As anticipated, the work group did not have control over research funding, or project priorities, so our efforts primarily consisted of information sharing.
- Although it was listed as a topic of interest in our IST-067 TAP/TOR, the group did not investigate urban communications issues related to Information Operations. It was discovered early in our

efforts that almost everything related to Information Operations is classified and the work group did not have the capability to handle, store, or process classified information.

- Although all of the work group participants were government sponsored, all members experienced some degree of difficulty and frustration in gaining access to technical information and data from researchers, agencies, and project offices.
- A key finding of the group was that there are in fact very few major research and development projects directly focused on tactical communications in urban operations even though it is a very important and extremely challenging sub-area of military communications. There is a great deal of communications related research and development being done on advanced technology topics such as software defined radio (SDR), cognitive radio, various waveforms, non-traditional frequency ranges, and mobile ad-hoc networks (MANET), which are likely to help with the issues involved with tactical communication in urban operations. None of these projects however, is directly focused yet on their direct application to communications in an urban environment.
- Several of the participating nations had small scale projects ongoing to test the suitability of certain frequency ranges, or examine the application of advanced technologies such as MANET for urban operations, but these projects are currently not considering the full three dimensions (surface, high-rise building, and underground) involved in urban operations or the interaction between these dimensions.

Chapter 2 – URBAN OPERATIONS – THE CHALLENGES FACED AND AN EXAMPLE OF THE LIMITATIONS EXPERIENCED

An example scenario for a military tactical operation in an urban environment would be the mission for a combined arms company team to secure a designated segment of a city. This operational space includes multiple dimensions as seen in Figure 2-1 [1]. This mission would include searching, clearing, and controlling each of the dimensions in the assigned sector: each room of each building in the area; pedestrian and vehicular traffic on the streets; and underground tunnels which might include subway lines utility tunnels, and sewer lines.

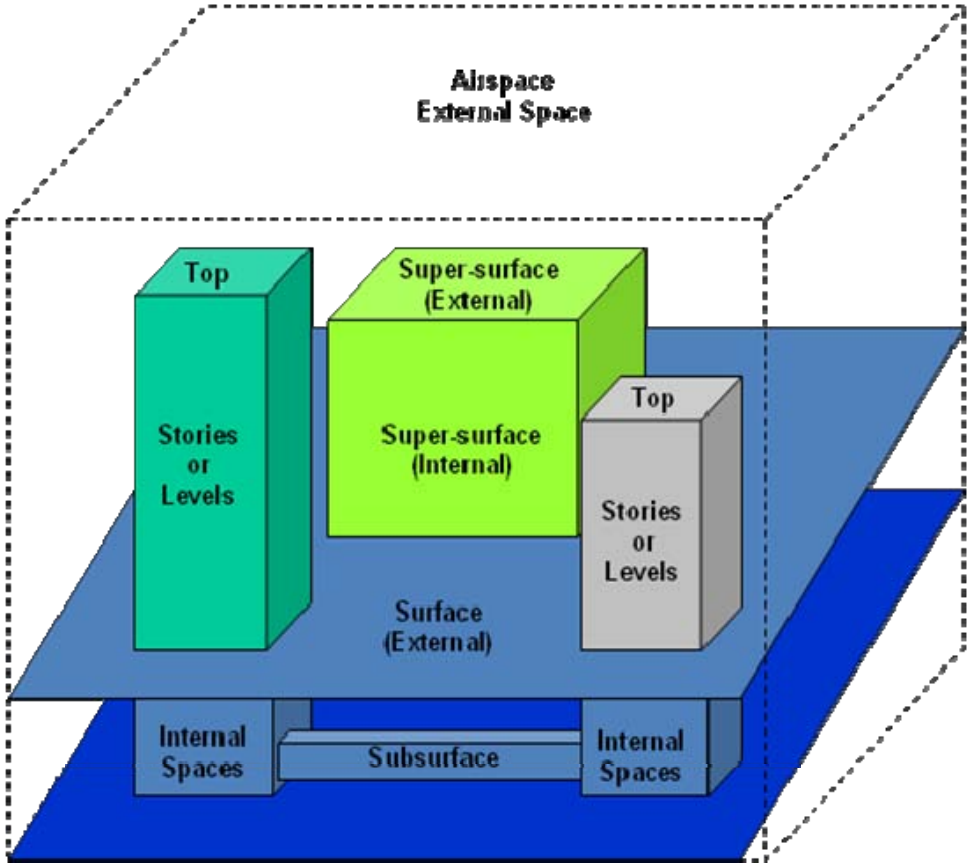


Figure 2-1: The Multi-Dimensional Urban Battlefield.

The Company Commander would typically establish a street level command post near a major intersection. With current systems and technology, and time and resources to apply appropriate lessons learned such as putting antennas and repeaters on rooftops, UAVs, and aerostats, the Commander may have very good communications with soldiers operating on the streets, and in the outermost chambers/ rooms of buildings. At the same time, the Commander is unlikely to be able to communicate with soldiers operating in the inner chambers/rooms of buildings or underground. Early in an operation before rooftop or aerial antennas and relays are in place, the Commander may be able to communicate only with those soldiers that have direct or almost direct line of sight back to the Commander.

Even given nearly unlimited time and resources the challenges of wireless communication in urban environments have not been fully solved by commercial enterprises or local governments. While mobile

phones work inside most buildings and in some subway tunnels due to massive infrastructure investments in towers and repeaters, it is still common to experience communications dead-zones.

Local government and emergency response (law enforcement, fire, rescue, etc.) communications radio frequency based systems are fairly similar to military communications systems and are much more prone to dead zones and limitations as compared to mobile phone systems, even if these are also cellular systems. Although radio frequencies are generally much lower than commercial mobile phone system frequencies, because of costs the geographical base station density of emergency response systems is lower. As a consequence, area coverage is generally less. In the United States, since the mid 1990s the city of New York has invested millions of dollars to integrate the communications systems of their many emergency response agencies, and to facilitate communications from subway lines, to street level, and into deep and high-rise structures. Despite many years of effort and a massive investment, many dead zones, barriers, and challenges still exist for this system. For example, while repeaters in subways may allow communication from the street to the subway, the system does not cover and support communication to/from utility tunnels and sewers. Figure 2-2 depicts the relays and technologies used in New York City and some of the remaining challenges in their system [2]. An example of an approach to solving this problem would be to use simulcast transmission such as that used by DAB or DTV which use synchronous transmission from many transmitters and long symbols. As stated previously, this report will not further discuss subterranean communications requirements.

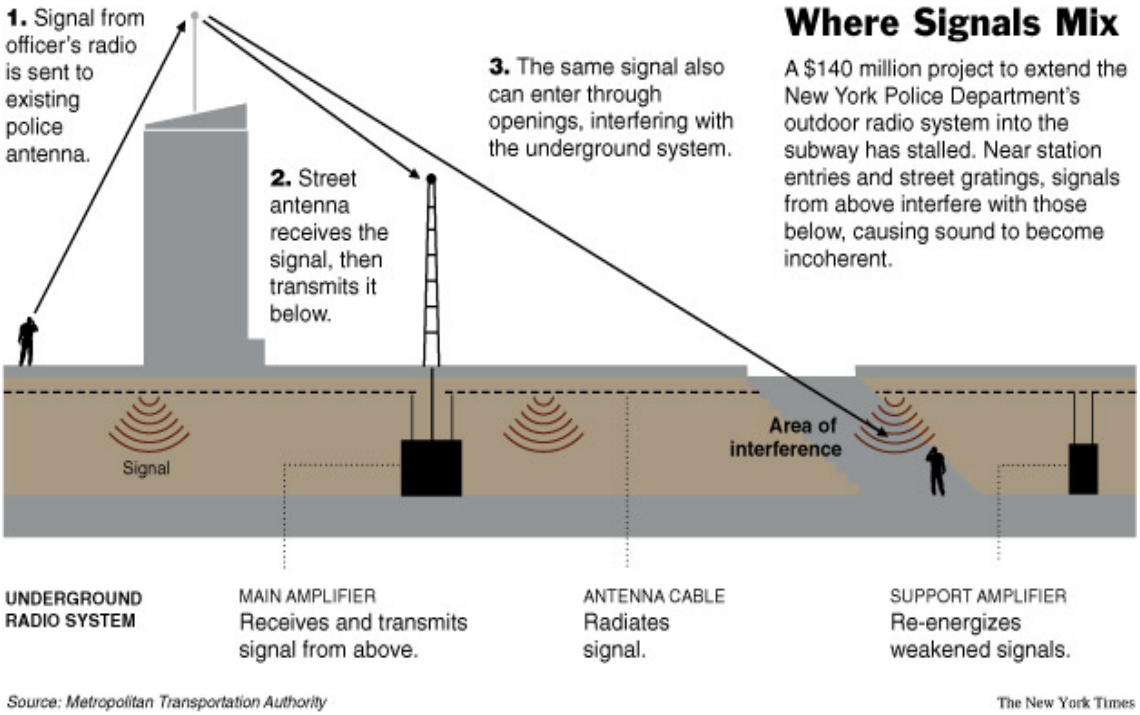


Figure 2-2: An Example Emergency Response System.

Chapter 3 – EFFECTS OF COMMUNICATIONS TECHNOLOGY ON URBAN OPERATIONS PLANNING (AND EVOLVING DOCTRINE)

Demographic studies indicate a vast increase in the number and size of urban areas throughout the world. Many future military operations will be taking place in urban areas. NATO forces must be prepared to conduct effective urban operations (UOs). Urban operations are combat and other military activities in an area of operations where significant defining characteristics are manmade physical structures, associated urban infrastructures and non-combatant populations [3].

Cities reduce the advantages of the present technologically superior force. The physical terrain of cities tends to reduce line of sight (LOS) and the ability to observe fires, inhibits command, control, and communications (C3) capability, and decreases the effectiveness of fire support. It also degrades logistics, and often reduces ground operations to the level of small unit combat. In addition, the constraints imposed by a need to minimize civilian casualties and preserve infrastructure further reduce present technological advantage and requires *novel* technologies such as: 3D mission planning, high-altitude platform relaying, robotics, etc.

Experience in these operations, and that of other military forces, shows that urban areas offer significant operational challenges across the range of military operations, but particularly for combat. The challenges inherent in urban operations are significantly different from other types of military operations, and their complexity affects all aspects of the planning and conduct of such operations. The great complexity of the urban environment requires military forces to pay particular attention to the unique and demanding requirements of operations in those areas. It is therefore imperative that commanders and staffs understand those requirements and consider them in the planning and conduct of operations in the urban environment.

Ground operations tend to become decentralized in an urban environment. The difficulties of communication and control that arise from the dispersal of units into buildings, underground passages, streets and alleys force command and control (C2) to devolve toward the smaller unit level (*power to the edge*). The presence and involvement of existing infrastructure in urban areas will impact military operations. Forces conducting urban operations face increased exposure to industrial interferences. Hence, soldiers and their commanders need sufficient information to act locally, based upon their mission objectives, reflecting the intent of the commander. Only the most critical information such as – status of their mission; unit health/condition; and their needs for support; must be reported to higher headquarters.

3.1 TYPES OF URBAN OPERATIONS

Urban areas are complex, dynamic environments. They are also, increasingly the sites of war, and military operations other than war (MOOTW). A single UO may involve both war and MOOTW missions concurrently. Urban operations are a sub-set of all military operations.

3.1.1 Urban Operations in War

Urban operations in war also cover a spectrum of possible actions. Ground combat – either offensive with the purpose of securing an urban area and destroying the adversary defending it, or defensive with the objective to deny the urban area to the adversary – is the most difficult and costly type of military urban operation. It is important that the commander consider forces and functions in unusual combinations and relations when planning urban operations, befitting the nature of the urban battlespace.

3.1.2 Urban Operations in MOOTW

Military operations other than war (MOOTW) increasingly take place in urban areas. These operations are typically categorized as either having or not having a threat or use of force. However, in many urban areas stability is tenuous at best, making the threat of some type of hostile action real in nearly all urban operations. Throughout the range of MOOTW, the same principles for conducting urban operations apply.

3.1.3 Multiple Operations

The nature of modern urban operations often results in different types of operations occurring simultaneously or in rapid sequence, sometimes in close proximity.

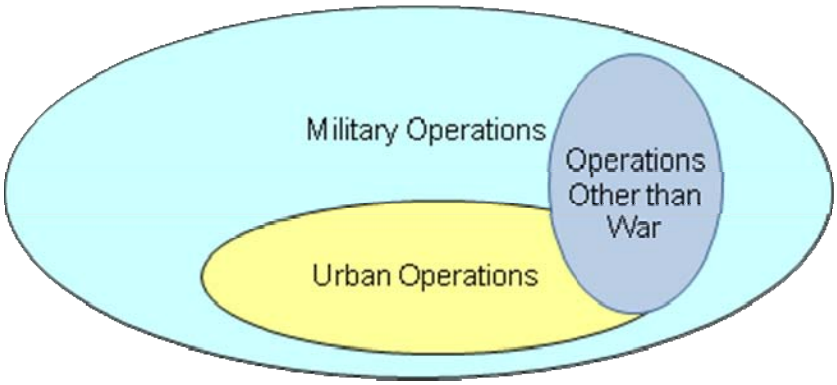


Figure 3-1: Urban Operations vs. Other Military Operations.

In the case of peacekeeping missions, peace enforcement, or disaster relief, cooperation with existing civil authorities and interoperability with civil communications infrastructure will be essential. All of this drives the development of new concepts of operations, requiring new tactical communication systems or novel ways of deploying or using existing tactical and (secondary) locally present communication systems.

3.2 PLANNING OF URBAN OPERATIONS

Planning for UOs generally follows the same basic process as planning for other operations. However, the challenges inherent in urban operations are sufficiently different and complex to require that commanders and planners give due consideration to urban requirements. The framework for planning and conducting UOs can be described in terms of the following activities: understand, shape, engage, consolidate, and transition: (USECT) [4]. These activities function as an interdependent, continuous, and simultaneous cycle and are applicable for urban operations across the entire range of military operations.

Urban operations strain the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities of military forces, requiring flexibility and innovation on the part of commanders and planners.

Planning and preparation of military operations in urban terrain can benefit from modern 3D modeling and simulation tools. These tools assist planners in evaluating various options, assessing advantages and risks, and producing tactical decision aids that improve situational awareness for warfighters and commanders. Modeling of urban terrain begins with mapping of the entire area. This process can use existing satellite images or aerial photos, or up-to-date information gathered during reconnaissance missions by manned aircraft or UAVs. Special high-resolution cameras and laser 3D terrain mapping payloads are used to collect the necessary images in order to enable accurate reconstruction of the buildings and surrounding

terrain features in 3D perspectives. These 3D models enable mission simulation rehearsals and detailed mission planning. Specifically, 3D models enhanced with propagation prediction models are able to identify communication dead spots.

3.2.1 Information Support

A large amount of information is needed to support forces in UOs. C2 is supported by an intelligence infrastructure with a reliable and secure communications and computer system that processes and integrates information and passes it to where it is needed. General information is often readily available on urban terrain, demographics, and infrastructure, but the precise and detailed information required to conduct operations may be more difficult to obtain. Task Group IST-046/RTG-018 "Command Center Challenges for Urban Operations" defined critical information requirements (CIR) for UO [13]. The list of requirements covers:

- Blue Force tracking;
- Mapping the city;
- Red and Brown Force tracking;
- Dynamic route planning (vehicles, soldiers);
- Real-time surveillance;
- Communications coverage (map and testing); and
- Building layouts.

Communications challenges for all CIRs incorporate:

- RF propagation and multi-path;
- High density and mobility of nodes and users;
- No stationary communications infrastructure;
- Jamming/interference;
- Radio equipment interoperability;
- Security (TRANSEC, COMSEC);
- Power supply limitations;
- High bandwidth applications (real-time video, etc.);
- Mobile routing;
- Frequency management; and
- Network management in mobile, urban environments.

Since civilian technology is commonly used for military operations, one great challenge is to avoid situations where a computer is waiting for a response from another computer, which is commonly seen as the "hour glass" in the Windows Operating System. Successful information retrieval is normally based on the availability of servers, proxies, and registrars in service oriented architectures and web services. As demand increases and these services become more sophisticated, there are multiple dependencies and single points of failure that may disrupt response time. There is a trade-off between information service quality and response time.

Solutions to communications issues that work in lightly populated, simple terrain will not work in the complex terrain of a heavily populated urban area. When the battlespace is an urban environment the requirements for communication become more difficult and more critical to provide to the individual

dismounted soldier, which becomes the focal point of operations. Providing adequate access to communication resources is essential to the successful completion of the urban mission. These operations usually require extensive intelligence support, including long range airborne and ground based observations, electronic intelligence and signal intelligence support by special mission aircraft and UAVs, etc. Forces are also equipped with the means of receiving data from, and exercising control over these systems, as part of their C4ISR capabilities. When operated and coordinated as integral parts of the operation, these C4ISR elements play a critical role in the security of the ground forces and the success of their missions. While maintaining a clear and constantly updated visual situational picture of friendly and hostile forces, these intelligence-gathering systems are also locating and reporting the target's status and activity.

Due to the cameras being located overhead (i.e. UAVs or rooftops) the transmission of the data is improved. However, not all objectives are accessible from overhead sources (i.e. tunnels, subway stations, etc.) and the built-up urban environment blocks the transmission of data.

While snap shot stills or video at very low frame rate may be most common at this time, near real-time imagery is becoming a critical element for the modern warfighter, but bandwidth resources available for the transfer of these video streams are usually limited. The transmission of the data for real-time surveillance of objectives, and routes of approach is anticipated to be primarily via high-bandwidth video links. Often the high-bandwidth data can be processed or compressed at the source, so as to minimize the communications requirements. New networks may provide much wider bandwidth, enabling multiple networks to coexist in the same geographical area, without unacceptable interference or degradation of Quality of Service (QoS). These wireless networks must employ robust, highly secure communications in order to protect this critical asset from hostile information warfare (IW) attack.

Imagery intelligence (IMINT) and signals intelligence (SIGINT) have often provided timely and fairly complete information to the commander, but both of these sources contain drawbacks when used to gather information in urban areas. IMINT can provide an accurate and up-to-date picture of the layout of a city, the functions of some structures, the location of communications sites, vehicular movement patterns, and other facilities and activities that can be viewed from the outside. However, IMINT has difficulty viewing the interiors of buildings and cannot view the subterranean areas of a city, and the sheer volume of movement makes interpretation difficult. Based on timely and detailed intelligence in Effect Based Operations there are two preferred methods of employment: "**networked snipers**" and precision-guided weapons. Suitable weapons include guided missiles of different types: laser homing weapons, **electro-optically guided weapons with "man in the loop" control**, and to a limited extent "fire and forget" autonomously guided weapons. Precision weapons are employed when targets are positively identified and confirmed by intelligence sources. The weapons can engage specific targets, such as positively identified armed personnel, vehicles known to be involved in weapons trafficking, an assembly of enemy commanders, etc., in real time.

Experience in urban operations clearly indicates that human intelligence (HUMINT) is essential in understanding the local behaviour and psychology, pinpointing locations, identifying targets, and developing situational awareness. However, the reliability of information gained from some of these sources can be questionable. HUMINT does not necessarily involve use of specialized operators. Troops and patrols constantly operating in an area can provide excellent and highly focused HUMINT if properly trained and equipped. Thanks to modern cellular communications, HUMINT does not always require direct contact between operators, agents, and the local population. Internet, wireless mobile phones, commercial phones, cameras, and SMS messaging have replaced the secret radio transmitters and Morse code of the past. These collaboration techniques enable HUMINT operators to recruit informers over the Internet, or via leaflets airdropped over an area of interest.

Commanders must guard against the mistake of failing to make a timely decision while waiting for better information. The urban environment complicates the problem of making critical information available to the commander, which can make the Commander's tasks more difficult.

3.2.2 Communications System Planning

Communications system planners are responsible for ensuring that the organization's communications network can facilitate a rapid, unconstrained flow of information from its source through intermediate collection and processing nodes to its delivery to the user. The nature of urban operations presents certain challenges to C4 and particularly to communications. Planning must take into consideration the differences between communications requirements and capabilities in urban operations and other operations, and the communications architecture should be modified accordingly, i.e. communication means should be adaptive. Existing infrastructure such as communication systems can both facilitate and hinder C4ISR. It may offer control and intelligence opportunities, but its absence will certainly add to the requirements of the joint force. Design and organization of joint force C4 architecture are influenced by decentralization, the three dimensional nature of urban battlespace, urban hindrances to radio communications, and the existence of an urban communications infrastructure [5].

The urban environment creates many unique difficulties for modern military operations. Without reliable communications controlling urban operations is extremely difficult. Communications become limited and unreliable due to multi-path reflections from walls, and electromagnetic obstruction by thick concrete and steel structures and, depending on the radio frequency, the reception of man-made noise caused by a wide range of devices emitting EM radiation. These effects cause degradation in the QoS for both voice and data networks, even at very short ranges. In addition to multi-path effects, multiple networks and large numbers of wireless devices operating over a wide frequency spectrum and in a confined area, cause severe interference. For instance GPS coverage is often limited to open areas due to interference and signal blocking, resulting in poorer coordination between forces and insufficient situational awareness, especially for operations in densely populated areas. New GPS receivers promise to reduce these limitations.

Urban areas contain varying degrees of communications infrastructure. This infrastructure may be relatively simple or it may be highly complex and sophisticated. The planners should determine the role and importance of key communications infrastructure elements for each phase and for the end state of the operation through an analysis of key facilities. This analysis examines each communication system individually and in relation to others and determines a course of action toward it.

In support of urban operations, C3 can involve the use of many different systems, from satellite links, wireless networks, and data-links to short-range, low power communicators. Broadband wireless networks provide the framework for net-enabled operations, allowing dissemination of a Common Operations Picture (COP) among all participating forces. Combat Net Radio (CNR) sets, now increasingly integrated into current combat vehicles already support integrated voice and data communications, facilitating direct links to databases and automatic reporting to battalion, brigade and division levels. Maintaining effective Command and Control in urban combat requires the use of efficient and effective networks supporting all combatants throughout the area, regardless of their location. These capabilities are not easily provided because electromagnetic propagation is severely degraded in such cluttered terrain, frequently limiting communications to short range, or even line of sight. These problems are so severe that multiple advanced techniques such as cognitive radio and hybrid multi-hop networks must be fully developed before they can be overcome.

To meet the need for connectivity and capacity in a constantly changing environment, it can be necessary to use civilian infrastructure alongside the military systems. The urban environment is typically heterogeneous considering radio resources, meaning that a specific area may be covered by several radio technologies simultaneously. Examples include civilian or military cellular systems, systems operating in non-licensed bands, and autonomous ad-hoc systems. A mobile node with multiple radio interfaces can communicate through two or more of these simultaneously. This gives the opportunity to choose the most suitable radio network and/or create backup channels via other radio links. There is no central management in heterogeneous networks. Well defined schemes are thus needed to manage handover for ongoing sessions when moving between different networks. One such handover scheme is described

in [6]. Operating in a heterogeneous environment also requires solving challenges such as handling the change of link qualities due to handovers; handling the mix of IP and non-IP networks; and methods for authorization and authentication.

Communications between neighbouring forces, sometimes even on parallel streets, may be limited and sporadic. Significant improvement in coverage can be gained by operating relay stations from airborne platforms or on high ground. Maturing aerostat technology and miniature man-portable UAV systems have been established as simple and reliable platforms for providing communications relay services.

Ground combat communications networks are usually operated in the VHF frequency band. This frequency band is relatively narrow and sensitive to man-made noise, and military radio networks do not use the available bandwidth as efficiently as current commercial systems. Consequent lack of available frequencies can limit the use of radio relays to overcome masking and interference. One solution to the problem is the use of Commercial-Off-The-Shelf (COTS) based communications systems owned and operated by military. Unlike legacy military radios or even the newer frequency hoppers, which require dedicated frequency resources for each network, COTS systems dynamically share a wide frequency band for optimal use of scarce resources. COTS systems are designed to provide deployable, reliable, and secure communications even under peak loads. In addition, most COTS communication systems operate in the lower UHF-band where susceptibility to man-made noise is much lower than at VHF, as previously discussed. Mobile subscriber networks, such as the TETRA based emergency communications network, provide automatic relaying of communications and data.

Communications networks can utilize ad-hoc communications to establish work-arounds between two points when direct communications are not possible. The network automatically establishes paths through other elements to regain the flow of information between all points and the central command post. These networks may include relatively simple wireless networks utilizing commercial “WiFi” protocols with restrictions on aspects like throughput per user, flexibility and radio range. In contrast, more advanced approaches including proprietary mesh networks which utilize advanced methods designed specifically to cope with the adverse effects of urban terrain may provide benefits such as better throughput and connectivity. Operating multiple high capacity links supporting video transmissions and control of remote systems requires the fielding of special data-links.

The decentralization inherent in urban ground operations requires the ability to communicate quickly outside the normal communications patterns. Because of the complexity of the urban terrain, situational awareness / common operational picture (COP) and battlespace visualization are very difficult.

The communications architecture should support representation of the entire battlespace: vertical and horizontal, exterior and interior, surface and sub-terrain, and airspace. In the final report of IST-035/ RTG-015 *“Awareness of Emerging Wireless Technologies: Ad-hoc and Personal Area Networks Standards and Emerging Technologies”* [24] authors suggest two strategies for the communications network architecture which are refined below along with a third hybrid approach:

- The first approach is the use of mobile ad-hoc networks not requiring a base station infrastructure in which mobile units (vehicles and dismounted soldiers) may communicate directly with one other, or by the aid of any other mobile. This type of network is normally referred to as MANET (Mobile Ad-Hoc Network) or wireless mesh networks.
- The second approach is the use of networks relying on an extensive infrastructure. In this kind of network two mobiles are unable to communicate unless both are connected to the infrastructure. Commercial cellular networks such as (2G) GSM, TETRA, (3G) UMTS, (4G) LTE and femtocells are examples of this type of infrastructure architecture.
- A third approach is to build a hybrid solution based on the first two approaches. An example would be to provide only limited network coverage using the expensive infrastructure based

solution and to use less expensive mesh networking for extending the coverage. This concept will be realised in the upcoming WiMAX amendment 802.16j.

Satellite and high altitude platform relay communications systems can provide the backhaul communication links necessary to support these approaches.

Radio communications are inhibited in the urban environment, where the proximity of tall buildings, power lines, and other urban features results in screening, shadowing, interference, and reduced ranges. Solutions include using systems relying on airborne relay or retransmission assets or using other platforms or equipment. The difficulty of communications in urban areas adds significantly to the equipment and manpower requirements of the forces engaged. Existing communications systems in an urban area may range from the very sophisticated to the rudimentary. However, all offer the possibility of use by the joint force to augment its communications capability, compensate for shortages, or meet early communications requirements during initial deployment. Particularly in MOOTW, the commanders may be able to make efficient use of existing communications infrastructures, from basic telephone lines (cellular) to video and data transmission networks. Depending on the type of operation being conducted it is possible to exploit existing communications infrastructures as primary or redundant means of communication. Commercial systems and components usually are not made with military requirements in mind, and may not always be suitable for such operations.

3.2.3 The Process for Communications System Planning

The process for communications planning is an integral part of operation planning. Commanders and planners must:

- Understand the mission, the mission environment, the intent, and concept of operations. Different phases of an urban operation necessitate different and distinct levels of communications system support.
- Determine what is shared, when, and with whom. Adapting a network to meet dynamic information-sharing rules advances modern warfighting operations in a multi-national environment.
- Understand the capabilities and limitations of available strategic, operational, and tactical communications system resources.
- Identify communications system requirements that exceed the capabilities within the engaged forces and coordinate (electromagnetic spectrum, equipment, or connectivity) any mitigating actions through appropriate channels.

Communications Planning Methodology includes five areas [8]:

- **Mission Analysis:** During mission analysis, communications system planners develop the communications system estimate and specified and implied tasks to be performed by operators and communications system personnel.
- **Information Needs Analysis:** Communications system planners work closely with all functional communities to develop Information Exchange Requirements (IER). IERs identify products to be transmitted and received, as well as the throughput, traffic load, latency and characteristics of those products (volume, classification, priority level, life time, etc.).
- **Interoperability, Compatibility, and Supportability Analysis:** Planners identify interoperability, compatibility, and supportability requirements and assess them against documented capabilities.
- **Capability Analysis:** Based on mission analysis, information needs, interoperability, compatibility, and supportability analysis, communications system planners identify the C2 systems and networks that can support the OPLAN.

- **Allocation of Communications System Assets:** After the template is developed functional component planners must examine all available resources and plan a tailored communications system. Through all phases of the operation, planners should utilize commercial systems where appropriate. Communications system planners shall centrally plan and manage, e.g. strategic and tactical SATCOM, electromagnetic spectrum use, and other C2 systems and networks.

The challenge of planning and conducting joint urban operations goes well beyond terrain consideration. The process of communications system planning should consider in particular:

- The integration of organic and non-organic military and commercial communications systems, combined and joint interoperability so the interfaces are transparent and the systems reliable.
- Horizontal and vertical C2 linkages.
- A balance between “push” and “pull” systems to meet the information needs of the force to prevent information overload.
- Balance the need for redundancy and flexibility with the available assets.
- Survivable communications system architecture that includes a diversity of communications routes, hardening and protection of equipment and communications sites, and availability of alternate modular communications system packages.
- Identify communications dead spots prior to the mission and adjust plans and procedures accordingly.
- Redundancy that provides diversity of paths over multiple (radio and fixed) means, with available replacement systems, and repair parts. The goal is the availability of a timely, reliable information flow.
- Use of available commercial networks.

These are typically manual tasks. Alternative functions such as dynamic spectrum allocation can be automatically carried out between radio nodes which form overlay networks on which limited spectrum resources can be coordinated and timely frequency leases issued. These networks may be centralized or distributed.

Modeling and Simulation of the communications system and the mission environment allows planners at all levels to design, analyze, and validate network architecture to measure and assess the flow of information throughout various types of networks (data, voice, video, digital and analog) and media (satellite, terrestrial, microwave, wireless, wired, fiber optic, and others). Simulation results provide quantifiable outcome predictions on planned networks or modifications to current networks.

Critical to success in communications system support to urban operations is electromagnetic spectrum management, which is a specialized area that relies heavily on systems engineering support and modeling to ensure electromagnetic spectrum dependent systems are mission ready and compatible within the intended electromagnetic environment.

3.3 COMMUNICATIONS TECHNOLOGY AND ITS INFLUENCE ON PLANNING URBAN OPERATIONS

When considering the influence of communication technology on planning UO there can be a wide range of impacts driven by different scenarios starting from typical use of classical radios (at present) to the use of advanced communications solutions (in the future).

The UO planning process, as stated in previous sections, regardless of the communications technology used, is based on USECT activities. Planning for UOs in contrast to other operations can utilize vast

amounts of information. Processing such large volumes of data will demand powerful tools. 3D terrain mapping and modern propagation simulations enable planners to identify communication shortages and dead spots taking into account possible intentional and non-intentional interferences. Those tools enable planners to assess whether projected communication networks meet IERs or not. When the requirements are not satisfied, the network should be reconfigured, according to available technology capabilities.

Awareness of available tactical and commercial communications capabilities and critical information requirements for urban warfare enables technology gap specification. Planners should consider the employment of additional components or communications systems to cover the gaps. Available military and commercial systems (MOTS and COTS) or existing civil infrastructure (especially in MOOTW) may offer an alternative means to satisfy requirements and may reduce costs as well as the number of deployed military assets.

It is worth noting that UOs in War have specific and severe information security requirements. In most cases this demand simply excludes the use of COTS products or existing civil infrastructure. Limitations on the use of certain technology can force additional organizational actions such as: change of the CONOPS or limitation of IERs (see Figure 3-2 below).

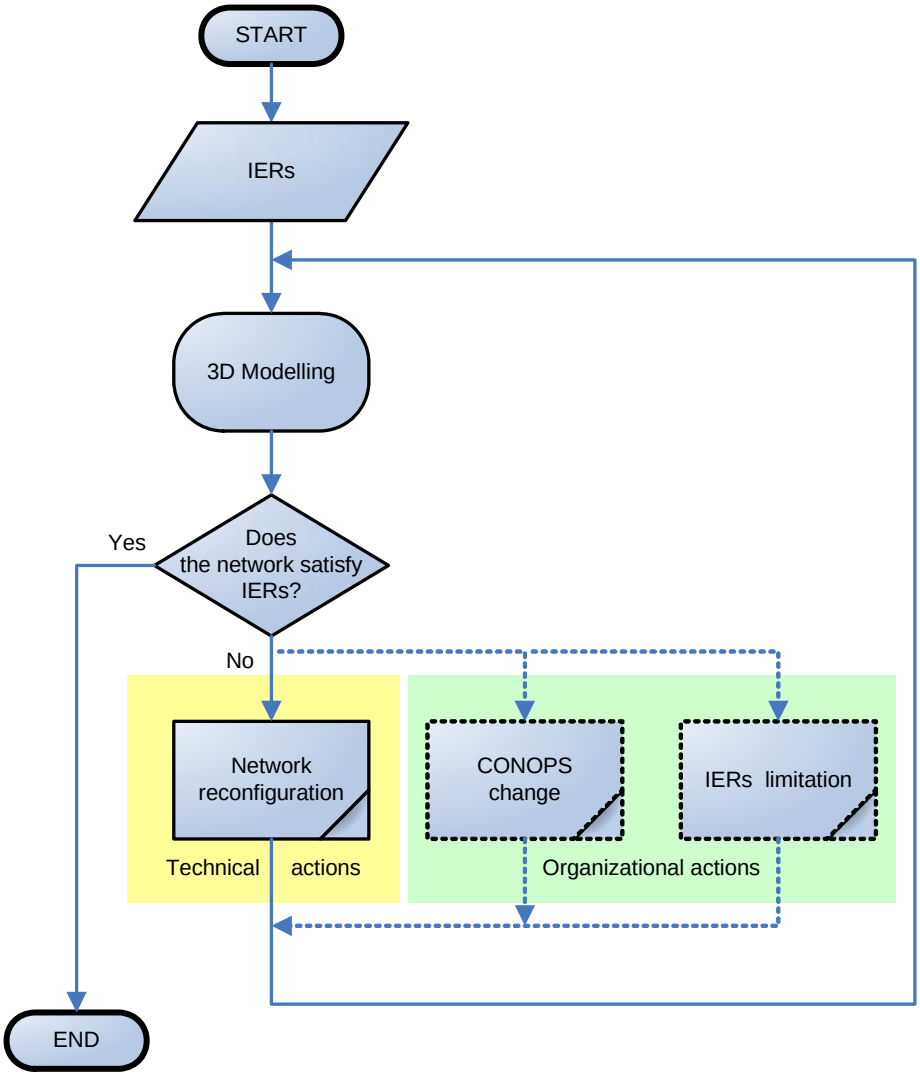


Figure 3-2: Communications System Planning Process.

If the available communications infrastructure is not able to support IERs and the probability of congestion or connection shortages is unacceptable, planners must decide to work within these limitations or add to the available infrastructure. Conducting operation in such conditions can cause coordination problems between units deployed in the urban environment, and even result in friendly fire. Problems with reliable information exchange can degrade the ability to conduct UOs according to NNEC/NCW for which seamless information sharing is crucial.

The urban environment is not predictable and tactical communications systems must be flexible enough to deal with dynamic changes. Automated network reconfiguration in case of topology changes is significant. This capability is necessary to ensure information (e.g. voice, stills, video) can be delivered in a timely manner despite organization or mission changes. Military forces must consider using existing civilian infrastructure to stay connected. The civilian infrastructure has been specifically designed for the environment, utilizing efficient waveforms and different techniques to deal with the problems of multi-path, fading, and intentional and unintentional interference coming from other systems. The ability to automatically avoid frequency bands occupied by other systems is advisable. Apart from this feature, frequency planning and management remains a great challenge.

Each well-designed automation mechanism built into the system allows planners to prepare schemes of operation with low probability of connection shortages. Exploiting such systems, especially broadband, will facilitate delivery of necessary information (e.g. Common Operational Picture) to urban teams increasing their situational awareness. Lack of infrastructure supporting external connections can be compensated for through self-configuring MANET networks which do not require base station infrastructures. MANETs can solve communication problems in small units deployed in relatively small areas of action (a few streets) where the number of terminals is limited. In the case of UOs where it is necessary to exchange information between units deployed in separated quarters or between units and their remote command posts, MANETs may require large quantities of nodes to provide an extended relaying capability. A heterogeneous MANET is an emerging concept for ad-hoc networks consisting of multiple bearers. If these heterogeneous MANETs are available in the future, the quantity of relay nodes necessary for communicating over longer range will be decreased.

Chapter 4 – URBAN COMMUNICATIONS EFFECTS ON CONOPS/TTP

For Military Operations in Urban Terrain (MOUT) it is not easy to identify how operational deployments will develop and progress considering the many aspects of Urban Warfare such as the irregularity of the enemy, presence of civilians, and the highly hectic physical environment. Instead, there are tactical concepts/ approaches that have been developed for this kind of operations in an effort to maximize impact and minimize the operational risks. Paradigm shifts with other than Urban Operations concern, e.g. [9]:

- Other Measures of Effect (MoE) than 'just' conquering territory;
- Bringing power to the edge, i.e. an operational approach level (introducing the "strategic corporal and junior leader");
- Handling a city as a comprehensive system-of-systems, requiring an enhanced operational framework (USECT: Understand, Shape, Engage, Consolidate and Transition);
- Combined arms approach (eliminating weaknesses by combining strengths in a 4-dimensional threat environment); and
- Requirement for enhanced situational awareness and enhanced precision to avoid fratricide.

It is considered instructive, in the framework of urban Concept of Operations (CONOPS) and Tactics, Techniques and Procedures (TTP), to relate communications to the context of a comprehensive, realistic military operation such as an amphibious landing operation with a disembarkation of troops in a harbor area that finally penetrate into a downtown or business area and a target object. The purpose of this is to identify in which specific ways communications may influence the CONOPS and TTP and hence mission planning.

This operation can be regarded as comprehensive and hence a relevant starting point for the communications in urban operations studies for the following reasons:

- The assumed "order of battle" of this operation is in agreement with the scope of this IST working group (battalion and below).
- A thorough analysis is required for such operations (i.e. as part of the "Understand" phase of USECT), pre-identifying urban and suburban choke points, key operational level nodes, systems, routes, etc. Also extensive logistic support has to be prepared at all levels and for all phases.
- The operation can be partitioned into a distinct number of phases, implying for communications:
  - A number of different physical environments are involved;
  - There will be a considerable variety of geographical unit densities and a large spread in distances between units;
  - Communication "need lines" will vary both in logical connectivity and required transmission capacity;
  - Out- and in-door battle situations are included; and
  - Different mobility and vulnerability levels can be identified.
- It reflects a combined operation in joint setting (land, sea and air).
- It will allow for a possible up-scaling, depending on the development of the conflict.

The following operation phases are important for consideration of communications aspects in Urban Operations:

1) Landing of infantry troops with light vehicles at the coast of the harbor area.
2) Displacement in the harbor towards the downtown/business area.
3) Displacement in the downtown/business area.
4) Dismounting of infantry troops and movement towards objects.
5) Entering objects to be cleared.

These phases will be described in more depth using the above facets as guidelines.

4.1 DESCRIPTION OF PHASES

4.1.1 Phase 1: Landing of Infantry Troops with Light Vehicles at the Coast of the Harbor Area

The key characteristic for this phase is the communication between landed units (vehicles) and the maritime command vessels approximately 90 km off the coast or by smaller platforms, nearer to land, as communication with the command ships will require specific additional measures such as relay ships or, more effectively, aerostats (mobile SATCOM may also be an option although there is significant end-to-end transmission delay involved) [10].

Radio line-of-sight propagation will take place over water. The required connectivity will be mostly point-to-multi-point from the sea due to the C2 that takes place. This can be voice and low rate data, both requiring limited bandwidth.

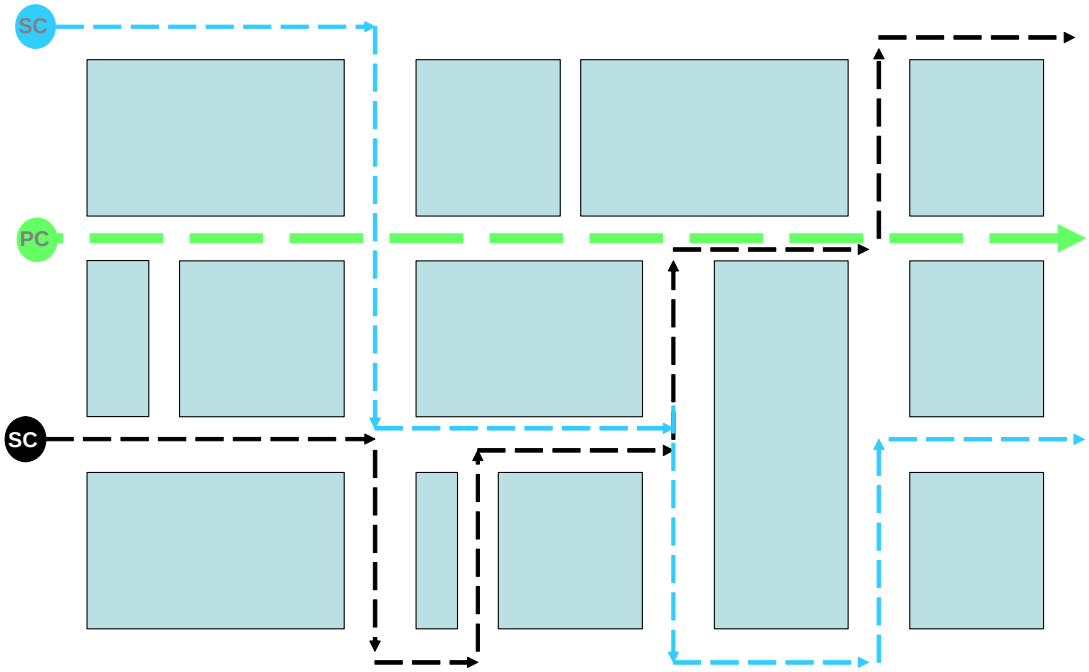
Some point-to-point feedback from the vehicular-mobile land troop commanders may be expected in the form of voice or stills, the last requiring low to medium bandwidth. It is assumed that detailed (static) 3D-map data have been made available before the landing as part of the mission preparation. These 3D-map data might also include propagation (computer-simulated) *dead spots* in the urban area.

In this phase, communication with helicopters is likely, providing fire and reconnaissance support from the air. This involves mainly broadcasts of data and high resolution digital images (yielding actual environmental data possibly combined with (static) geometrical data) from these platforms to the vehicles.

4.1.2 Phase 2: Displacement in the Harbor Towards the Downtown/Business Area

In this phase, mutual communication between the vehicles is also to be expected, mainly by voice and data. The vehicles will be initially scattered over a certain coastal line and will advance in a semi-random pattern usually referred to as *satellite patrol*.

The essence of this approach is illustrated in Figure 4-1.



PC = Platoon Commander; SC = Squad Commander

Figure 4-1: Satellite Patrol Principle.

In the *satellite patrol* concept a commander maneuvers forces through an urban environment towards the final object rather than move straight toward it. In Figure 4-1 this is a platoon commander who displaces in the direction denoted by the green line. Units under his command will displace in the streets as "satellites" around the platoon commander's route. These units are referred to as satellite units. In the example of Figure 4-1, the satellite units are represented by two squad commanders, moving along the paths of the blue and black lines, respectively. The principle is applicable to vehicular and dismounted unit displacements. Further, note that paths of the platoon commander and of the satellite units may even cross occasionally.

Advantages of this approach are that:

- A considerable presence is suggested by a limited number of military personnel;
- The rather unpredictable movements of the satellite units will confuse the enemy and will reduce the vulnerability of friendly forces; and
- The urban area of coverage is enhanced. In effect, relative small incidences and threats may be resolved *en route*.

Some disadvantages of satellite patrol are that it requires synchronization and planning. The fact that no units are abreast of others and are in constant movement with respect to each other will complicate radio communications: this will, e.g. frustrate the use of terrestrial pre-disposed relays and of (somewhat) directional antennas. In general, the geographical unit density is limited and mutual distances may vary considerably (e.g. to several blocks).

The physical, industrial environment of the harbor may, depending on radio bands used (HF, VHF, UHF, SHF), induce radio signal interference from *manmade* sources. As a general rule, manmade noise will increase with decreasing frequency.

While communications line-of-sight may be consistently blocked, there remains a requirement for the exchange of situational awareness data consisting of friendly unit locations and potential threats. In more advanced systems, the sharing of stills or even of moving images may be envisaged. Sharing implies the use of broadcasts, however selectively addressed messages may not be excluded [11]. It is likely that satellite patrols, especially vehicle mounted patrols, may be guided and supported from the air. This implies that the communication between the vehicles and helicopters as stated in *Phase 1* will continue in the second phase.

4.1.3 Phase 3: Displacement in the Downtown/Business Area

The characteristics of this phase are quite similar to those of *Phase 2*. It is assumed that satellite patrols will continue, only in a changing environment. A primary difference between the harbor location and the downtown/business area is the presence of more built-up structure, more blocking, and narrower streets, being urban canyons for radio propagation. Also the characteristics of manmade noise may vary due to other equipment and densities of these disturbance sources in the vicinity of the units. The built-up area size usually is about 8 x 8 km on average.

At the end of this phase, the initial entry troops will reach objects where they can consolidate and erect a (possibly multi-national, e.g. NATO) spearhead HQ and prepare for the clearing of vital objects. At this level it is also assumed that eventually, during more stable periods, opportunities will exist for specific CIMIC functions and hence communication and co-ordination via the HQ. This will require the means to be interoperable with NGOs, local public safety and civil government entities [12].

4.1.4 Phase 4: Dismounting of Infantry Troops and Movement Towards Objects

In this phase, mobility has decreased because of the dismounting of infantry troops. The platoon and company command vehicles stay behind in relative safe areas. The requirement for helicopter fire and command support may be assumed. However, this depends on environmental possibilities such as building density and heights.

In general, movements will take place in a satellite patrol pattern, close to objects to maintain coverage from sight and fire. Although the environmental effects on radio communication will be comparable to those mentioned in *Phase 3*, the transmission power will generally be reduced because of the use of handheld radios. Hence, transmission range and/or robustness will be decreased in spite of lower mobility.

Sewer systems may serve, if possible, as alternative roads in this phase. The obvious advantage is that maneuvering friendly forces are far less vulnerable to attack. However, (apart from other drawbacks such as the lack of mobility, escape routes and gas hazards) radio communications is severely affected underground. Specific measures such as deploying repeaters are required. Besides this, displacement through underground systems is not preferred since one may realistically assume that the hostile elements know underground system deployment details and may wait for their opponent at certain locations. Units will only displace underground if strictly necessary.

Dismounted soldiers will communicate mainly by voice for coordination and command. They may occasionally exchange still images and (automatically) position updates for the purpose of situational awareness and a common operational picture on command levels. Easily controllable ‘light’ data applications may not be excluded. In general, the dismounted soldier has to concentrate on the tactical situation which implies that any requirements to pay attention to ICT device control should be kept to a minimum. There are nevertheless situations, such as providing medical assistance to a unit member, in which certain data applications are of such high value that they are expected to be used in spite of a high threat situation.

In conclusion, maintaining communications between platoon and company command vehicles and dismounted soldiers is difficult, but vital.

4.1.5 Phase 5: Entering and Clearing Objects and Buildings

This phase will be characterized by extreme danger and high risk due to the many uncertainties involved in entering buildings, lack of information about enemy location and intention, and the possible presence of Improvised Electronic Devices (IEDs). The situation is made worse by the lack of visual overview and the fact that the soldiers entering buildings have no direct logistical or fire support. It would be a considerable help if building layouts could be made available prior to the action, however this generally will not be guaranteed. Such information could also reveal propagation *dead spots* since there is possibly poor radio propagation within the structures as a result of the structure geometry and building materials used, hence complicating communications and localization.

The squad members entering structures need to devote *all* attention to the threats of the situation and have no opportunity to actively control communication devices. Voice communication traditionally is the prime requirement. However, enhancement of situational awareness and common operational picture could be accomplished if the user interface allows for an uninterrupted focus on the current situation (e.g. projection technologies of immediate, simple data). Since there is generally a lack of visual overview in this situation, the hazard of *blue-on-blue fire* is considerable. Therefore, situational supporting data in the form of squad members' positions may be a crucial means to prevent fratricide.

Image transmission may also not be excluded in this phase, however it is assumed that this information has to be gained and transmitted to the commanding levels automatically for their judgment and operational picture. Commanders may use this information to command and control the soldiers by voice. The direct interchange of images between squad members is not considered likely in this phase.

4.2 GENERIC REQUIREMENTS AND BOUNDARY CONDITIONS

The following requirements and limitations caused by the physical environment, operations and equipment are generic in nature and may apply to multiple operational phases and conditions:

- Connectivity should be maintained while soldier is flat on the ground or during crawling in a sewer pipe (problems with conventional antennas in military frequency bands).
- Dismounted soldiers and their commanders wear thick operator gloves, restricting their ability to control devices [11]. Also for a direct control, distributed device control (i.e. over the equipment and/or body) may be preferred.
- In military light vehicles, space and power supply are usually limited. This compels the use of small-sized radio equipment and may limit transmitter power and hence range.
- It is debatable if radios used in Urban Operations should feature TRANSEC and COMSEC *at all times*. This requirement depends on several aspects such as the life time of exchanged information and the probability of jamming in specific urban environments. Like many other protection measures, advanced electronic protective measures (EPM) usually increases volume and weight and decreases mobility of dismounted soldiers.
- Due to close proximity to the enemy, friendly forces will be vulnerable to radio-direction finding which would expose their location to the enemy. Classical countermeasures are directional antennas and short on-air times. With respect to the last, there should be optimal use of source and information coding [13].
- Because of its considerable operational value [14], not only vehicles, but also future dismounted soldiers are likely to be equipped with body-wear sniper detection systems [15]. These will

require robust communication links to share the detection information with other squad members and with the platoon commander. This in turn will require local data fusion with positioning systems and a body-wear network to aggregate the information together with data such as bio status information to the squad radio.

- Radio equipment of dismounted soldiers should be physically robust, i.e. shock-, water-, wear and tear proof.

As a countermeasure against malfunctions, the use of back-up communication means has also to be considered in UOs in spite of several boundary conditions such as volume, weight and power consumption.

4.3 CONOPS/TTP CONCLUSIONS

In documenting the phases of the comprehensive case scenario several considerations have been identified that all refer to finding the balance between the consequences of enabling radio communications and the necessity to adapt the CONOPS and TTP accordingly:

- **Satellite patrolling** by vehicular and dismounted units offers multiple operational advantages but may restrict geographical unit density. The use of pre-disposed relays and directional antennas that may be required to obtain radio range and throughput that are normally limited by urban environment propagation characteristics. Airborne relays may form a solution to this problem.
- The need for services supporting situational awareness and special protection measures (e.g. sniper and gunfire detection) in all phases of urban operations requires robust radio communication links and sufficient transmission capacity and therefore enabling technologies such as source coding, a carefully selected frequency band, modern radio multiple access techniques, etc.
- **Unit agility** is generally required but frustrated by increased radio equipment volumes and weights. Specifically, batteries and their operation time are of concern in this respect.
- **Interoperability** (joint, combined and with NGOs) is to be considered in many phases, requiring flexible radio waveform interoperability. The possible use of SDR is of relevance at this point.
- The general use of sophisticated **EPM** is to be considered against the drawbacks of increased equipment volume and weight and reduced mobility, operability and interoperability and the protection by less sophisticated measures (e.g. short on-air times).
- **Displacement** of dismounted soldiers underground provides physical protection but is generally avoided. If units displace underground, this will require specific ad-hoc communication measures (e.g. “breadcrumb” relays and flexible antennas).
- **Protection against IEDs** ignited by own radio systems is a major general concern both during indoor and outdoor operations. At this point, the wide spread use of separate detection devices seems the only answer to this problem.
- **Extensive mission preparation** using 3D-information on target areas and objects require a considerable investment, usually involving intensive and laborious intelligence. However, this may not only reveal locations of physical danger but may also predict possible radio dead spots in outdoor and indoor environments, which may then be avoided.

Chapter 5 – REQUIREMENTS VERSUS AVAILABILITY OF CURRENT AND FUTURE SERVICES

Most people live in cities and therefore the market for communication systems is tailored for urban use. There is rich opportunity for COTS equipment suited for urban operations. There are however special requirements for military communications systems for urban operations.

Today's military standards are EUROCOM based and those of the future are Internet Protocol (IP) based. Modern radios must be equipped with an IP stack for communicating even if the radio signaling waveforms are far different than the data signal format of IP, because wire or fiber optic channels using IP are likely to be used as relays or repeaters for radio signals.

To meet the demand of life and death critical tactical operation, future radios must be able to communicate information and share data classified up to NATO SECRET. In the following tables, some of the most important findings of NC3A report TN 1246 [12] relevant for urban operations, are summarized.

Table 5-1: Wireless Communication Requirements by Traffic Type (from [12] p. 27)

Traffic Type	Quantity/Data Throughput	Security (Highest Requirement)	Quality of Service	Remarks
Voice	Low	COMSEC / AJ	1	
Voice/Stream	High	COMSEC / AJ	1	UAV reconnaissance streams, etc.
Blue Force Tracking / Operational Awareness	Low/Medium	COMSEC / AJ	2 / 3	FS to support combat, e.g. ICC, LC2IS, JCOP
Targeting	Low	COMSEC / AJ	2	Weapon release authority may be from high in the chain of command
Core Data Service	Medium	COMSEC / AJ	4	Email, file transfer
Functional Services	High	COMSEC / AJ	3 – 4	FS to support non-combat forces such as Intel, e.g. LOCE and logistics, e.g. ADAMS, LOGFAS

In almost every case, confidentiality of the traffic transported over the air in a wireless communication system is required, the exceptions usually being for liaison with non-NATO entities. It was noted that the level of protection which must be provided may not have to reach NATO SECRET (NS) or MISSION SECRET (MS). In current operations, the requirement for some degree of confidentiality on CIS networks and the availability of equipment inevitably leads to the creation of NS and MS networks in addition to unclassified networks. It was also noted that in operations where there was no requirement for SECRET level CIS and where traditional cryptographic equipment could not be used, e.g. support to the African Union, alternative CIS operating at a lower level of classification had been used successfully. Future capabilities within NATO make the support of alternate security domains to the conventional NU and NS/MS possible. This is already in evidence during transitions in current operations, e.g. NATO HQ Sarajevo, where a NATO RESTRICTED network will be provided as the main secure network, with NS "islands" being deployed only where necessary.

According to [12], jamming protected (transmission security) waveforms must protect both signaling and traffic while in transit over the air since in common scenarios, protection against hostile jamming is considered a necessary requirement. It is the conclusion of this group that encryption and anti-jamming for the lowest tactical levels is subject to debate because of the relative low benefit compared to the cost, due to the extremely short life time of the information. Additionally the danger of the compromise of the whole crypto system if a node should be captured may outweigh the benefit of encrypting the data. Finally, inclusion of encryption makes international interoperability much more difficult. While anti-jamming capabilities are theoretically always desirable, given the unlikelihood that the enemy has sophisticated jamming capabilities or will use them at this level, the benefit of adding anti-jamming capabilities are presumed to be outweighed by the costs. The observations within this group are that unintentional interference from multiple sources that are normally encountered in an urban environment seems to be a greater threat than jamming.

There is no requirement for low probability of intercept (LPI) and low probability of detection (LPD) communication in the NATO scenarios. Where LPI would be necessary or beneficial these forces and capabilities would be provided nationally without any direct requirement to interoperate with Alliance or Coalition forces.

Quality of service has been used to describe not only the common ‘QoS’ concept employed by wired communication networks but a wide sweep of characteristics including transmission delay and reliability. Any real-time service such as voice will require a QoS of 1 in Table 5-2.

Table 5-2: Quality of Service (from [12] p. 30)

Quality of Service	Example of Service Type	Number of Locations Required	Level Throughput
1	Voice Real-time video	All	Mainly low
2	BFT, Targeting Combat functional services	Many	Mainly low
3	Combat support functional services	Some	High
4	Email Combat support service functional services	Some	Medium

The operational community noted that the timeliness of information was highly dependent on the specific operation being undertaken although this was difficult to characterize. Future wireless communication systems must be capable of supporting the most stringent timeliness requirements.

The range required in wireless communications in most of the scenarios was in the region of a few kilometres, with longer ranges required for connectivity back to the HQ and other forces outside the Battle Group in question. See Table 5-3. The communication range will have a significant impact on the system and technical views of the architecture.

Table 5-3: Wireless Communication Requirements by Range (from [12] pp. 29-30)

Range	Characteristics	Throughput	Security	QoS	Required	Typical Application
< 1 km	Urban Non-LOS	Low	COMSEC	1 3	All All	Voice, Targeting BFT
1 – 20 km	LOS	Low Medium High	COMSEC	1	All <Most <Many	Voice, BFT, Target CS, FS, Target Video, FS, Target
> 20 km	BLOS	Low High	COMSEC COMSEC	1 1 4	Few Few	Voice, BFT Voice, BFT Targeting, Voice BFT, CS, FS
A/G/A (low speed)	LOS	High	COMSEC	1	Few	Video, Targeting CS, FS

It was noted by the operational community that there was also a requirement to provide a wireless capability to support initial entry operations where a small spearhead HQ (20 – 100 personnel) needed to be established quickly and before a more stable "long term" solution could be provided. Such a capability would afford speed of response, flexibility and eliminate the disadvantages associated with wired systems. It was recognized that this required a risk management approach to security which is contrary to the current risk avoidance policies. However, such a wireless HQ capability for initial entry forces would fall within the responsibility of NATO or a single nation.

Chapter 6 – SPECTRUM IMPLICATIONS: NATO POLICY ON THE USE AND MANAGEMENT OF THE RADIO FREQUENCY SPECTRUM

The total radio frequency (RF) spectrum available for all civilian and military radio communications is a limited natural resource [16]. Use of the spectrum by the military is impacted by economic, public policy and technical factors, which affect decisions on who may use the spectrum. Demand for spectrum has increased considerably due to global communications technology use, driven by the increased role of information in society. This issue is not unique to tactical communications for urban operations, but spectrum management is especially important in an urban environment because the density of spectrum use is likely to be far greater in an urban setting.

Military RF spectrum requirements are driven by command and control needs, and include wireless devices on all tactical levels, including strategic planning support, training in the homeland, and in-theatre use. The common military uses are applications such as fixed and mobile radio communications, radio-navigation, radars, identification, weapons systems functions, meteorological aids, medical support, and finally useful COTS equipment. Notice that these applications operate over a variety of range, and hence transmit power levels.

Coordination of RF use and related management tasks is becoming extremely complex, as compared with the legacy way of doing business because of the unpredictability of spectral use by dynamic network architectures. The political visibility of RF issues is also increasing, in part because the economic value of the radio spectrum is increasingly visible to the public due to the proliferation of commercial wireless services.

NATO requires the safeguard of continuous and adequate spectrum access by nations to ensure that Allied defence responsibilities are met. In some alliance countries military spectrum management is conducted in coordination with civilian authorities, although the military frequency managers are generally responsible for specifications of requirements for military users. The spectrum management needs of NATO must be supported by individual nations. This may therefore be in conflict with the increased commercial value of radio spectrum.

The NATO Frequency management sub-committee (FMSC) is a coordinating body that harmonizes the military use of spectrum within NATO and partners, and develops NATO positions on ITU congresses, amongst other responsibilities.

SMADEF-XML [17] is the NATO approved format used to exchange information related to the spectrum management process. The purpose of this standard is to specify the format of each data element and the structured messages to be used when exchanging each category of spectrum management information. This paves the way for automatic exchange of frequency management data between computers, simplifying international cooperation in urban operations.

6.1 THE STATE OF THE NATO UHF BAND

This section gives an overview of the current state. For more in-depth information see [18] and [19]. The NATO UHF band is 225 MHz – 400 MHz, and is the primary band for air-to-ground-to-air (A/G/A) communications. This band is also part of the anticipated band for future networking waveforms. The dominant occupiers of the band are identified in Table 6-1.

Table 6-1: NATO UHF Spectrum Users

A/G/A	33%
Wideband Mobile	25.8%
SATCOM	9.6%
Civil	8.7%
Navy	6.7%
Other	16.2%

The availability of the NATO UHF band (225 MHz – 400 MHz) is an 'indispensable' asset for NATO and partners, and erosion to commercial or civil use is an ongoing concern. The efficient use of this band is important for the military users to defend continued availability.

The current allocations are for predetermined channelization. With the incorporation of varying bandwidth wideband systems (in increments of 1 MHz and possibly 5 MHz), this poses a coordination problem with existing users of the band, in that legacy users must have the investment and capabilities in equipment protected.

There is a desire for NATO to improve the spectral efficiency of air-traffic control voice systems (STANAG 4205), reflecting the improved spectral efficiency of voice codecs, and to demonstrate efficient use of existing military spectrum allocations. The current channelization is 25 MHz, and it is proposed to go either towards 8.33 kHz (as some civilian systems use – see [19]) for a spectral efficiency increase of 3. This presents major technical problems for tactical waveforms due to the increased LO stabilization requirements on equipment for very high aircraft velocities, and the feasibility of this has been investigated with negative result. Also being considered is an alternative TDMA approach where multiple users use the same channel using an access-coordinated protocol.

Another concern is the loss of the top 20 MHz (380 MHz – 400 MHz) to TETRA, which reduces the total band size by roughly 10%. This has an operational impact to the frequency hopping waveforms, in a reduction of spreading gain, and the essential lowering of anti-jam (AJ) robustness.

There is an investigation for a planned US satellite MUOS to use wide bandwidths over the entire 224 – 400 MHz band. Compatibility studies are underway.

6.2 ESSENTIAL SPECTRUM REQUIREMENTS

The scope of spectrum users within NATO is illustrated in the following non-prioritized unofficial list:

- Long-haul strategic networks;
- CNR;
- Air operations;
- WAN including maritime and amphibious links;
- SATCOM networks;
- Air surveillance;
- Weapons systems;
- Sensor systems;

- Radio-navigation;
- Identification;
- Meteorological;
- Medical support; and
- Others.

6.3 CCEB SPECTRUM TASK FORCE (STF) TASKING BY CCEB EXECUTIVE GROUP

The CCEB is the combined communications and electronics board, and is within the organizational structure of the military alliance of Australia, New Zealand, Canada, United Kingdom and United States, generally referred to as AUSCANNZUKUS. The spectrum task force is an ad-hoc study group that has prepared a report and advice for the CCEB Executive Group about the impact of new networking communications systems, including systems to support net-centric warfare, and cognitive radio (CR), on the planning and management of radio spectrum. For more on CCEB see [20].

6.3.1 Background and the Future of Spectrum Management

The demand for RF spectrum is increasing at an unprecedented rate within the defence community. The growth of the numbers and spectrum demands of conventional systems is leading to a lack of spectrum. In addition, the explosion of wireless devices found in net-centric systems (both communications devices, data transfer networks such as ISTAR, and sensor networks) will exasperate the problem. If left to follow this natural progression, military operation capabilities that rely of radio spectrum will be in jeopardy. This will also result in the inability of commanders to plan and complete the types of missions expected to be supported by future net-centric warfare capabilities.

Communications resources of the future will adapt to the variation of operational scenarios during an operation, in order to optimize utilization of scarce radio spectrum. This leads towards more dynamically configured communications networks, which can evolve their configuration and networking according to the flow of the military operation, the varying propagation, and the EW environment. In this type of network, spectrum is required, and accessed in an unpredictable manner, which is incompatible with current spectrum management practices that designate specific blocks of the band to specific users.

There is the increasing realization within the military spectrum management community that change is coming due to the evolution of how radio networks are designed. It is also understood that significant risk to operational effectiveness will be present if change is not initiated in the near term in anticipation of wireless networking technologies.

The CCEB envisages a future state around the year 2025 where spectrum access to fixed allocations is made efficiently, military capabilities are enabled by flexible spectrum access while using the minimum amount of spectrum as practical, and battlespace management, network management, and information management are integrated in a way that devices can optimally access spectrum dynamically to meet operational need.

The scope of the effort to reconfigure the management of spectrum is described according to the topical areas: spectrum management for operations, adaptive RF technology, coalition spectrum architecture, spectrum management and network management convergence, acquisition process, security, tools, information management techniques, regulation, and awareness.

Important conclusions are related to properties of future communications systems, change in management techniques, improved management of information transfer requirements within a network, and raising awareness of these spectrum management challenges within the defence community.

6.3.2 Impacted Areas

The major conclusions of [20] are categorized in the following ten subject areas spanning all parts of military preparations and operations.

6.3.2.1 Spectrum Management for Operations

The focus of this topic is the need for changes in policy and practice to ensure that spectrum management inputs are provided in the early stages of the operational planning process, reconciling warfighter spectrum requirements with spectrum availability. It also discusses changes to the spectrum management organization required to support operations in the face of spectrum congestion. The benefit of closer interaction of the spectrum community and operational management is the integration in battlespace, resulting in a spectrum management capability that ensures availability and use of spectrum.

6.3.2.2 Adaptive RF Technology

Adaptive RF technology is being introduced or developed in the military and civil domains for communications, RF sensors, and EW applications. The introduction of this technology has the potential to enable flexible, efficient and dynamic access to spectrum forming one element of the capability needed to meet future operational requirements and to help mitigate spectrum congestion. It will also introduce new spectrum management challenges and potentially introduce new vulnerabilities. It is important that appropriate RF technology is adapted to operational needs while ensuring that the technology remains manageable in the coalition spectrum domain. It is also essential that any new technological vulnerabilities are understood.

6.3.2.3 Coalition Spectrum Management Architecture

A Coalition Spectrum Management Architecture should be developed and maintained representing the basis for a transition plan to meet the future challenges. This architecture will represent the coalition aspects of spectrum management and the interfaces into national architectures. The benefit of having an architectural plan is that it provides the understanding required to implement change, while minimizing the unforeseen consequences.

6.3.2.4 Spectrum Management and Network Management Convergence

Military wireless communication is necessary for a variety of critical applications. As reliance on the network and the information exchange requirements increase, so in turn will spectrum demand. Mitigation of this demand requires that the network needs and spectrum use needs be dynamically optimized. This will be achieved by convergence of spectrum management and network management processes becoming increasingly closely coupled and will entail the introduction of appropriate technology. Failure to converge the SM and NM processes will result in sub-optimal use of the spectrum and ultimately spectrum congestion will impair operations.

6.3.2.5 Acquisition Process

The development of spectrum dependant military capabilities must be undertaken with spectrum availability and constraints considered from early feasibility studies and through to eventual disposal. This consideration of spectrum must account for the most severe spectrum environment in which the

capability will be deployed. Then, the probability of equipment compatibility in all operational environments is maximized, and instances of degraded performance and unavailability of key capabilities are reduced.

6.3.2.6 Communications Security

Communications security imposes constraints on connectivity, particularly in coalitions, resulting in inefficient communication topologies. Security devices and measures also impose significant overheads on data flows that are increasingly useful due to the introduction of modern IP cryptography.

6.3.2.7 Spectrum Management Tools

Interoperable tools are needed that address the various spectrum management processes, importantly by way of using a common data exchange format. This ensures that all the data required to manage spectrum can be readily exchanged between national staffs. In addition there will need to be new and better automatic tools to allow effective management of spectrum in a more dynamic and complex environment. Without tool interoperability effective spectrum management in a more dynamic RF environment will not be possible. Different national needs will require different tools so the most appropriate interoperability mechanism is a common data exchange standard.

6.3.2.8 Information Management Techniques

Increasing spectrum demand in the communication domain is driven in part by increasing data exchange requirements. Mitigating spectrum demand can be achieved by reducing the volume of data that needs to be transmitted. This can be achieved by adopting information management techniques to compress data, to ensure data gets to the correct recipients efficiently and eliminate redundant information transfer. Recent operational experience suggests that only a small amount of the information transferred in the battlespace is ever used. Capabilities that generate data rarely consider spectrum constraints, and so fail to adopt appropriate data processing techniques.

6.3.2.9 Regulation

International and national regulatory issues must be addressed in order to develop positions to coherently influence national administrations in respect of the ITU and WRC, while cognizant of national changes in the member states and trends in regulation in operational regions. The radio regulations must be automated to allow effective spectrum management. WRC and ITU influence is important to countering pressure on military spectrum resource from the worldwide civil community. The radio regulations underpin much of the spectrum management process, and the ability to assimilate the regulatory data into spectrum management tools will enhance effective management.

6.3.2.10 Awareness

Awareness of spectrum risk and appropriate consideration of the spectrum impact of decisions in the military community is currently inefficient. It is essential that the spectrum community pursues every opportunity to raise awareness. Failure to raise spectrum awareness will lead to sub-optimal military decision making in this respect and to the continued lack of spectrum consideration in capability acquisition.

6.3.2.11 Conclusion

It should be realized that the density of spectrum utilization is most severe in urban environments. Spectrum management must be central to all communications planning and military operations. Demands on the NATO UHF Band are increasing rapidly and we will soon reach a point where it is saturated and

unavailable for some users. This band is regarded as the most useful for urban communications, and should be very carefully managed during urban operations. The NATO CCEB suggests that dynamic configuration of spectrum is not foreseen until 2025, however enablers are under development. There are other groups working on related issues such as the IST-035 Task Group on ‘Military Cognitive Radio’. Cognitive radio is discussed in the next section of this report.

Chapter 7 – URBAN COMMUNICATIONS TECHNICAL APPROACHES AND ISSUES

The following sections identify and briefly describe important research and development areas that are likely to have, or at least have a potential, for impacting tactical communications in urban operations. Some of the material, programs, or approaches described are from or about the efforts of a single nation, but all have potential applicability across NATO.

7.1 FREQUENCY ASSIGNMENTS AND COGNITIVE RADIO

7.1.1 Frequency Assignments

Traditional frequency assignment is often referred to as "Command and Control Frequency Assignment". An assignment (of a radio frequency or a radio frequency channel) is defined as an "Authorization given by an administration for a radio station to use a radio frequency or radio frequency channel under specific conditions." Each country will have one authority, or alternatively several coordinating authorities, for assigning frequencies. The authority determines the availability of the desired frequency or spectrum sub-band, the consistency with regional and international agreements, and verifies that the assignment will not cause interference with other users. The frequencies or spectrum sub-bands are typically assigned for a significant amount of time. As an example, in Norway this varies from 5 to 20 years for some services, or the assignment applies as long as the frequencies are needed or until the authority determines that they are not longer available for the particular user or communications provider.

Frequency assignments as a general rule must be in accordance with "The Table of Frequency Allocations" as published in by the International Telecommunication Union (ITU) and incorporating the decisions from the World Radio Communication Conferences. An allocation (of a frequency band) is defined as an entry in this table. The table lists frequency intervals and allocated services in these intervals in each of ITU's geographical regions. This type of frequency assignment is beneficial for the licensed spectrum users in that it provides a high availability of their assigned spectrum resources and a low level of interference.

Some frequency management authorities have to some extent responded to the higher degree of dynamics of telecommunication, e.g. by providing spectrum licenses instead of more specific system licenses, by allocating unlicensed bands where several user groups may coexist, by having spectrum auctions, and by allowing sub-licensing of spectrum. The overall picture of frequency assignment is still a very static one. Assignments are long-term in accordance with allocations that are very-long-term. Spectrum is not released when not being used short-term or medium-term, and since the assignment process involves manual administration and decision processes the specific assignment may involve a significant waiting period for an applicant.

In military operations, national forces must co-operate with other nations and coordinate the use of frequencies with multiple national authorities. For this purpose, a database of all frequency assignments in an area will be needed as well as a terrain propagation model for the area.

7.1.2 Cognitive Radio

A cognitive radio (CR) has the ability to sense and to some extent reason about its environment and adapt its communication properties like protocols, modulation, transmission power and spectrum usage to its context, where the context includes the spectral environment it observes. A CR may also learn from the results of its adaptations. CRs may have different levels of cognitive capabilities typically organized in

nine levels of capabilities. CRs may also have different levels of adaptation possible among their communication properties. These features will be most useful for military operations since it will make deployment in hostile or unknown terrain much easier. This applies to UO as well as non-UO.

CRs are seen as a means to increase spectral utilization, in that CRs may detect, or collect information about, unused or underutilized spectrum and may use this spectrum on an ad-hoc basis, possibly co-existing with other services in the same spectrum band.

A main CR technical problem is that of 'hidden nodes.' Even if a CR, here termed A, detects that a certain portion of the spectrum is available, some radio station B, may still receive interference from A. This may for example be due to B being undetectable due to its transmission level, or due to B being a receiver with a clear transmission path to its transmitter companion C, C however not being detectable from A. The hidden node problem may be compensated for somewhat, though not eliminated completely, by having additional spectral sensing equipment at elevated positions (such as an airborne platform), or by exchanging spectral sensing information in a network of CRs, also known as distributed spectrum sensing.

Significant computational and reasoning capability is required by the CR. Key tasks include making intelligent autonomous decisions in locations where the CR coexists with legacy systems and networks of other CRs, and where at the same time the topography is complicated, implying a high probability for hidden nodes.

The IEEE 802.22 is referred to as the first wireless standard based on CR. The IEEE 802.22 Working Group develops Physical (PHY) and Medium Access Control (MAC) layers for a CR-based Wireless Regional Area Network (WRAN). These 802.22 devices are to co-exist, as unlicensed units, in spectrum bands allocated to Television (TV) service, wireless microphones and some other Private Land and Commercial Mobile Radio Services (PLMRS/CMRS). The 802.22 devices form point-to-multi-point networks, where one base station (BS) manages associated Consumer Premise Equipment (CPEs).

In 802.22, the BSs and CPEs are responsible for not disturbing the other licensed users of the spectrum bands. Several techniques and mechanisms are planned to facilitate this, including:

- A distributed sensing mechanism takes into account a combination of measurements both at the BS and at the CPEs to obtain reliable spectrum occupancy figures. CPEs are planned to perform spectrum occupancy measurements at start-up, and are also instructed by the BS to perform periodic measurement activities.
- Low sensing thresholds for the spectral occupancy measurements.
- Calculation of a keep-out region around DTV transmitters.
- Defined timing parameters, e.g. the detection time for the detection of a licensed user.
- Beacon transmission from wireless microphones is drafted in the standard as an option, as wireless microphones are difficult to detect due to their low RF output power.
- A Spectrum Usage Table is maintained either by the operator or by the system itself. The table may record frequency, location, and operational characteristics of PLMRS/CMRSs.
- Measures are incorporated to avoid interference between neighbour WRAN cells to ensure successful coexistence.

The problem in cities is the lack of non-LOS operation due to the obstruction of tall buildings. The use of the relay feature in IEEE 802.16j may therefore be especially useful for UO.

Through these mechanisms, the 802.22 system takes great care to avoid disturbance of other licensed users, achieved through the computational complexity of building up and using information about the

surrounding spectral environment. However there is still a small risk of disturbing undetected hidden nodes, e.g. wireless microphones without beacons.

The Dynamic Frequency Broker (DFB) [21] is a computer automated service which is responsible for assigning frequencies to radio nodes within its geographical area. This is expected to be very useful for tactical military operations enabling smooth frequency assignment among various national radio users in an area. In order to take into account consequences to radio nodes in local or distant geographical areas, DFBs coordinate their assignments by forwarding and dealing with frequency requests as needed.

7.2 THE CELLULAR CONCEPT IN URBAN OPERATIONS

A number of nations are examining the use of commercial, cellular mobile phone concepts for tactical communications. Recent military missions have shown an increasing need for resilient radio connections in urban operations for obtaining situational awareness within relatively small units. Radio connections in urban environments suffer from object blocking and man-made noise. Both phenomena vary highly in time, also due to unit agility. Research [7],[22] showed that the radio connection availability of The Netherlands land force's current combat net radio (CNR), PR4G, is unreliable for radio connectivity between vehicles at the levels of platoon and company. Also, it has been concluded that a cost effective approach, answering the radio communication requirements at these levels in urban operations, is far from evident.

In 2005, the so-called cellular approach was introduced as an alternative urban operations telecommunication solution in place of current CNRs and possible future ad-hoc networks [7]. Although military aspects and further technical implementation possibilities of this idea have been discussed, not all have been quantitatively addressed. However, the requirement for quantification and further analysis of this approach emerged to assess its feasibility. The research program designed to explore the issue is described in some detail in Annex A of this report.

One major disadvantage of the cellular approach that remained (both qualitatively and quantitatively) unsolved is that of lack of EPM. The attached report therefore deals with the feasibility of the cellular approach with a focus on adding some limited EPM capabilities. Other communication security aspects will not be considered. For a complete feasibility assessment of the cellular approach, additional aspects such as required protection measures (physical, redundancy), training and education, maintenance, materiel overhead and logistics (required assets and transport of central components to and within an area-of-operation) and management and control will be important but are outside the scope of the current project.

The study deals with mobile radio communications in a built-up urban environment at the level of platoon and company vehicles, reflecting a worst case for terrestrial radio communications. A mutual comparison between several cellular system alternatives within the 400 and 900 MHz bands is made, reflecting short-term candidate systems in frequency bands that are promising in urban environments. For this study, a vehicular satellite patrol scenario has been selected with one company and multiple platoon vehicles. The mutual *maximum* distances between platoon and company vehicles are assumed to be approximately 2 km. The maximum distance of the (vehicle-mounted) base station to the platoon and company vehicles is taken to be 8 km.

The EPM is achieved by dynamically controlling the base station antenna footprints during the course of military action. Values for base station antenna height, azimuth and elevation beam widths are determined that will allow all vehicles to remain within the base station antenna foot print. To enable the adaptation of beam widths, current vehicle coordinates are assumed to be automatically (periodically) transmitted to the base station. Specifically, realistic base station antennas and their attainable gain values have been identified for the 400 MHz and 900 MHz systems. The COST-231 Extended Hata model and a geometric analysis have been applied.

7.2.1 Initial Results

Results of the project to date indicate that in terms of range and coverage in urban areas, 400 MHz systems outperform 900 MHz systems. However, more directivity can be realized for 900 MHz systems than for 400 MHz systems, resulting in an EPM that is approximately 5 dB larger for 900 MHz systems. Also, addition of MIMO and SIMO enhancements to improve EPM threat resilience is more practically realizable for 900 MHz systems.

Even with base station antenna gain enhancement techniques and considerable base station antenna heights, current results indicate that in most cases satisfactory performance will only be feasible with the use of airborne relay platforms such as aerostats and UAVs. If required for a tactical scenario such as displacement phases prior to the battle phase in the built-up areas, satisfactory range performance can be obtained if an airborne node is introduced. In this case, if the effective antenna height exceeds approximately 2 km, the elevation footprint becomes more predictable and smaller. However, this means that its size has to be checked to ensure it does not become lower than the minimum elevation footprint operationally required. Distances in suburban and open space areas clearly indicate that the use of airborne relay platforms at high altitudes also provides the possibility to use one radio communication means in the vehicles. In this case, separate long distance transmission means could be used as a backup.

Of specific interest are the numerical results summarized in the Table 7-1 below.

Table 7-1: Initial Results for Cellular Concept Tests

Results: ranges and base station antenna heights h_b

	400 MHz		900 MHz	
Environment type	Regular ant's (6 dBi)	Enhanced dir. ant's (17 dBi)	Regular ant's (18 dBi)	Enhanced dir. ant's (22 dBi)
Urban	h_b = 140 m for 8 km range	h_b = 40 m for 8 km range	h_b = 250 m for 8 km range	h_b = 175 m for 8 km range
Suburban	14.5 km	14 km	17.5 km	18 km
Open	54 km	45 km	76 km	75 km

7.2.2 Follow-On Results

To further investigate the feasibility of an enhanced radio range using an airborne relay, follow-on activities have been carried out by the Netherlands in the form of a measurement campaign [23]. The measurements aimed to identify the receive quality in extremely complex urban environment and simulating disadvantaged users, realizing a high-altitude transmit location and assess the attainable single-link ranges (i.e. from airborne relay to mobile station or vice versa). In this measurement campaign an airborne relay payload has been simulated by deploying a radio-antenna system on top of a 100 m radio relay tower, situated in a built-up, dense urban area. The platform height represents a tactical platform, such as a Vertical Take-Off and Landing (VTOL) device. This height will not violate legislation, nor will it provide problems for the uplink transmission link budget (assuming a transmit power of app. 1 Watt). A mobile receive station followed pre-defined routes in the nearby built-up dense area (app. 250 m) and in a distant built-up, more sparse area (app. 6 km) from the transmit location, respectively.

At the mobile receive station the received signal powers (within a 25 kHz regular bandwidth), the (man-made) noise levels (no signal transmitted) and the corresponding positions on each route walked have been measured and stored. From the measurements the SNR (Signal-to-Noise ratio; actually the carrier-to-noise ratio in these measurements) has been derived for each measurement band, position and route (one for each location). Measurements have been carried out in both military VHF (30 – 88 MHz) and military UHF (225 – 400 MHz) bands to compare the performance of the current PR4G combat net radio with a current TETRA-based radio or a future UHF radio:

- Measurement results show that airborne relay considerably increases the attainable ranges for both VHF and lower-UHF in urban environments of several signatures (dense built-up to more sparse with lower buildings). End-to-end ranges via an airborne relay proved to be in the order of 10 km (for manpack transmit powers). Airborne relay therefore could successfully extend both the range of current combat net radios that proved to be less than 1.5 km at ground use [23] and the range of lower-UHF (normally much less than 1 km). The limited propagation of VHF signals has also been noted in Bowman studies (Annex C of this report), even without deployment of relays.
- The sensitivity of VHF radio versus the poor sensitivity of (lower-) UHF radio for man-made noise has been clearly demonstrated.
- In general, changes of both VHF and lower-UHF signals could well be related to changes in surrounding building patterns. Signal decays due to entrance of corridors and going around corners have been clearly demonstrated. Also the receive signal increase in case of blocking *absence* (i.e. LOS condition) has been identified. In particular, lower-UHF signals have shown a more agile pattern of receive power (i.e. with a high density of dips) because of their sensitivity to multi-path compared with VHF signals.

7.3 MOBILE AD-HOC NETWORKS

The purpose of mobile ad-hoc networks (MANET) is to allow for wireless multi-hop communication by means of self-configuring networks of mobile routers and hosts connected by wireless links. MANET networks are intended for situations where no pre-established communication infrastructure is available and the topology of the communication links may change dynamically, but can also be used to enhance or replace infrastructure based networks. Each node of the network should be used as a router to forward data to destination nodes that are not within radio communication range. Thus, one of the important aspects in a MANET is the routing mechanism. MANET concepts are being explored for many military applications. A more complete report on the topic of military MANET efforts is attached as Annex B of this report.

Depending on the field of application for the MANET there are several challenges to be considered. The NATO IST-035/RTG-015 Final Report [24] discusses these military applications:

- Dynamic and rapidly changing topology;
- Low available bandwidth;
- Lack of a centralised entity;
- Large network diameters;
- Existence of unidirectional links;
- Scaling up problems; and
- Security considerations for these shared medium access networks.

The report summarises: *"These issues require that a routing protocol for a mobile ad-hoc network should be self starting and self organising, which provides the multi-hop, loop free paths to the required*

destinations in the network. Because of the mobility of the nodes, there should be a mechanism of dynamic topology maintenance, and rapid convergence of the protocol should be assured to stabilise the system. But the daunting task is to make it all possible using the minimum memory and bandwidth resources, and minimal overhead for data transmission. It is also required from these protocols to be scalable to large networks."

As the above statement implies it is hardly achievable to design a MANET protocol which fulfils all requirements and meets all challenges. It is therefore of crucial importance to identify the set of (urban) scenarios a MANET protocol should be used for and create a specialised MANET protocol tailored to these scenarios. Such a specialised protocol adapting to different urban environments and conditions does not need to meet all the requirements as a generic protocol would have to and may therefore be easier to design.

Annex B of this report first describes the current status of mobile ad-hoc network and then attempts to identify relevant issues that have to be addressed in future research. While the importance of these issues may vary depending on the scenarios the MANET protocol is used for, theses issues should be regarded whenever a MANET protocol is created. In the following we will provide a brief summary of the annex.

7.3.1 Current Status of Mobile Ad-Hoc Networks

Until recently the MANET subject was mainly discussed in the academic area. Today, it is becoming an important topic in commercial products and solutions. One reason for this development is that the MANET protocols are no longer seen as competitors to infrastructure based networks but as a complement, e.g. they can be used to connect several WLAN access points in a so-called Wireless Distributions System (WDS). Since there are many applications for a MANET, there are many different products and also different technological approaches. In some products the end user is part of the MANET and in other products, e.g. in a WDS scenario, the end user is only connected to a MANET node and therefore uses the MANET as a transfer network.

Currently, a multitude of public projects exist where ad-hoc networks are used or where it is planned to use them. The applications range from public safety to public access. It can be assumed that the use of ad-hoc networks will further increase in the near future, so that military ad-hoc networks may benefit from the progress in non-military projects. Projects in the area of public safety may especially be of interest to NATO.

Regarding the standardization of mobile ad-hoc networks some approaches from IEEE and IETF exist. As an example the upcoming extension 802.11s will introduce wireless mesh networking to the 802.11 wireless LAN standard. The current draft specifies that conforming radios must support the Hybrid Wireless Mesh Protocol (HWMP). This protocol uses a proactive component to discover a root station, which can be used to provide the mesh network with access to the Internet or other networks.

In the context of wireless metropolitan area networks the IEEE Working Group 802.16 (WiMAX) provides the standard extension 802.16e which allows for mobile recipients. If the network nodes are used in the mesh mode they can form an ad-hoc network. Due to the usage of TDMA a time synchronisation of the nodes is necessary, but this also renders Quality of Service classes possible. Using TDMA requires that the medium access is controlled. There are two different scheduling mechanisms for the mesh mode: centralised and a decentralised approaches. In the decentralised approach the right to send data is agreed in the two hop neighbourhood of a node. The upcoming standard extension 802.16j will add multi-hop mesh networking capabilities and aims at increasing the overall coverage by adding meshed base stations. In the discussed scenarios the base stations are assumed to be stationary, so it questionable whether the meshed nodes of the final version of 802.16j can be mobile or not. All in all the two extensions make WiMAX more flexible and strongly increases the value for urban operations due to the added multi-hop

capabilities. But it has to be taken into account that the relay stations are assumed to be stationary and that a solution with mobile relay stations may be preferable.

7.3.2 Important Issues for Future MANETs for Military Use

Current approaches for mobile ad-hoc networks often include only some aspects which are important for military use. While the aspect of a dynamically changing network topology is taken into account by most of the routing protocols, few protocols take the dynamics of link quality into account. Additionally aspects like transmit power control, data encryption and many others are only addressed by some approaches and there is currently no MANET approach which takes all important issues into account. Depending on the application area the following aspects are considered to be of special importance for future MANETs for military use. Security aspects, as they are regarded in other networks must be reconsidered to take the special challenges of MANETs into account. This includes specialised Denial of Service (DoS) attacks (e.g. against the network topology), hiding traffic flows and network topology even though a shared medium is used, efficient encryption key update mechanisms and intrusion prevention and detection mechanisms with low bandwidth links. Beside the security aspects, solutions for Quality of Service (QoS) and congestion control must fulfil high demands due to rapidly changing network conditions. Additionally scalability issues have to be taken into account so that high data rates over multi-hops become available. Last but not least in many application scenarios an efficient multi-cast and broadcast support for MANETs is desirable to reduce the load on the network.

7.3.3 Readiness of Mobile Ad-Hoc Networks for Support of Urban Operations

In their current state MANET solutions are only of limited use for military purposes. While there are some civil commercial products available, these products cannot fulfil all requirements of military communication systems. Current approaches for standardization, as observed in the IEEE and IETF, may be beneficial for the future development of these products, but it cannot be expected that all important issues will be solved in this context. It is therefore of special importance for future research that the exact requirements for different military scenarios are determined and specialised protocols for these scenarios are developed. Although not all of the above issues must be solved for every scenario these issues can be used as a guideline for the research which has still to be done and should be intensified. We expect MANETs to be of increased use as more and more of the requirements are fulfilled and included in products. Short-term solutions may therefore be applicable in some urban scenarios but we might expect major usability improvements for urban scenarios in the long term, especially if all network nodes should be mobile and security considerations are important in these scenarios.

7.4 SOFTWARE DEFINED RADIO

The expected urban environment will demand extreme flexibility in tactical communication systems, including rapid switching between available waveforms and frequency bands in response to rapidly changing operational conditions. SDR promises to be critical in solving these issues especially in combination with other advanced technologies such as MANETs.

Many future developments of military wireless communications involve multi-modal devices connecting to a wide range of different networks such as the commercial 2G, 3G, TETRA, WiFi and WiMAX. The underlying architecture needed to achieve this is termed Software Defined Radio (SDR). An SDR is characterized by a reconfigurable and programmable hardware platform which allows loading the specific waveform signal processing functionality as a software programme. In the future, this flexibility might enable more efficient use of the available spectrum through rapid deployment of the latest radio technologies. To date the defence industry has been the main sector to explore SDR. It is, for example, being deployed as part of the U.S. Joint Tactical Radio System programme. Industry is now showing an

interest in using SDR in radio network base stations. SDR could help to make the equipment more 'future proof', allowing operators to more rapidly introduce new technologies and services and allow manufacturers to fix problems and add new features post-manufacture.

SDR technology facilitates implementation of some of the functional modules in a radio system such as modulation/demodulation, signal generation, coding and link-layer protocols in software. This helps in building reconfigurable software radio systems where dynamic selection of parameters for each of the above-mentioned functional modules is possible. A complete hardware based radio system has limited utility since parameters for each of the functional modules are fixed. A radio system built using SDR technology extends the utility of the system for a wide range of applications that use different link-layer protocol, modulation and demodulation techniques.

7.4.1 Key Features of SDR Technology

7.4.1.1 Reconfigurability

SDR allows co-existence of multiple software modules implementing different standards on the same system allowing dynamic configuration of the system by just selecting the appropriate software module to run. This dynamic configuration is possible both in handsets as well as infrastructure equipment. The wireless network infrastructure can reconfigure itself to a subscriber's handset type or the subscriber's handset can reconfigure itself to a network type. SDR technology facilitates implementation of future-proof, multi-service, multi-mode, multi-band, multi-standard terminals and infrastructure equipment.

7.4.1.2 Connectivity

SDR enables implementation of air interface standards as software modules and multiple instances of such modules that implement different standards can co-exist in infrastructure equipment and handsets. This helps in realizing global roaming capability. If the terminal is incompatible with the network technology in a particular region, an appropriate software module could be installed onto the handset (possibly over-the-air) resulting in seamless network access across various geographies. Further, if the handset used by the subscriber is a legacy handset, the infrastructure equipment can use a software module implementing the older standard to communicate with the handset. Depending on the complexity of the waveforms relative to the implementation technology simultaneous operation of multiple waveforms may be possible. This will be of considerable operational value in UOs as it enhances connectivity and saves room aboard platforms. In practice though, antenna interfacing and possible co-location interference problems are to be considered. In addition, if the SDR platform offers the capability to operate multiple waveforms simultaneously, it can be used in a network as a relay (e.g. for range extension using the same waveform) or gateway (translator between different waveforms).

7.4.1.3 Portability

Portability defines the ease with which a system or component can be transferred from one hardware or software environment to another [25]. SDR facilitates implementation of open architecture radio systems. End-users can seamlessly use innovative third-party applications on their equipment's as in a PC system. This enhances the appeal and utility of the system.

7.4.1.4 Interoperability

Interoperability defines the ability of two or more systems or components to exchange information and to use the information that has been exchanged [25]. If the same waveform is running on several SDRs (possibly of different types, vendors, etc.), interoperability needs to be guaranteed among those SDR platforms as well as to legacy systems. Such interoperability allows improving the efficiency of cooperation between the forces of participating nations in combined and joint missions.

7.4.2 The Future of SDR Technology

A software-defined radio (SDR) system is one in which the baseband processing as well as DDC/DUC modules are programmable. Availability of smart antennas, wideband RF front-end, wideband ADC/DAC technologies and ever increasing processing capacity (MIPS) of DSPs, Field-Programmable Gate Arrays (FPGA) and general-purpose microprocessors have fostered the development of multi-band, multi-standard, multi-mode radio systems using SDR technology. In an SDR system, the link-layer protocols and modulation/demodulation operations are implemented in software.

If the programmability is further extended to the RF section (i.e. performing analogue-to-digital conversion and vice-versa right at the antenna) ideal software radio systems that support programmable RF bands can be implemented. However, the current state-of-the-art ADC/DAC devices cannot support the digital bandwidth, dynamic range and sampling rate required to implement this in a commercially viable manner.

Current drivers such as future-proof architectures, seamless integration of new services, multi-mode equipment and over-the-air feature insertion in military and commercial radio networking systems have resulted in widespread interest in SDR technology. The technology can be used to implement radio network infrastructure equipment as well as radio equipment and other end-user devices.

SDR in the military domain has been developed through several governmental programs, e.g. SpeakEasy I and II, and the ongoing JTRS program. The key result of the JTRS programme is the Software Communication Architecture (SCA). The SCA defines an open, distributed, object oriented software architecture which allows separating the waveform application from the operating environment and the hardware platform. In theory, both parts can be developed independently facilitating the portability of waveform applications and the interoperability of hardware systems.

SDR has promised flexibility in enabling multiple waveforms to be run simultaneously on one radio hardware platform, life-cycle cost reductions through generic and standardized hardware platforms, to solve interoperability issues among allies by allowing cooperation waveforms to be loaded onto the equipment, and to be an enabler for ad-hoc networking waveforms suitable for the future information grid.

After 2.5 billion US$ spent in the US development programs between 2003 and 2007 [26], and after 10 years of standardization efforts on the SCA, the radios offered still fall short of the above goals: SCA-compatible SDR platforms are still expensive. Exchanging waveforms is still not easy, made difficult by domain- and nation-specific security components and interfaces, by other domain-specific non-published interfaces, through waveform implementations being tailored for specific processing elements, and intellectual property rights especially to the legacy waveforms.

SCA-compatible SDR platforms are heavier and consume more power than their conventional counterparts which are just programmable. Networking waveforms have been developed for SCA-compatible SDRs, but these waveforms probably would have been less costly to implement and could have run with less power-consumption on conventional equipment.

The progress of SDR depends on several key issues [27]: The evolution of processing technology relative to the waveform and encryption demands. With static waveform processing capacity requirements, processing technology advancements will eventually allow SDR equipment to be lighter and less power-consuming. If waveform requirements increase at the same rate as in the civilian sector however, it will be demanding for processing technology to keep up with the requirements. To solve the SW exchange problems, further political, security and standardization efforts are needed, as well as technology advancement, e.g. in the field of model driven development. Securing the openness of the SCA or equivalent and their associated APIs is of vital importance.

7.5 SMART ANTENNAS

Smart antenna technology has the potential to significantly increase the efficient use of spectrum in wireless communication applications within urban environments by intelligently directing the communications signal at the user. The technology has the potential to increase the range and capacity of transmission equipment, reduce interference with other devices, and selectively reduce jamming.

Smart antennas have been used for many years, notably in defence radar, sonar, and military communications. Low volume production of such systems has meant that the cost of smart antenna technology has remained high. Significant advances in for example, processing power, are now bringing the technology closer to being commercially viable in the near future for civil communications applications.

However, there are a number of issues that are restricting the widespread adoption of smart antenna technology, including:

- **Technical** – Mainly hardware constraints;
- **Business** – The current relatively high cost of deployment often outweighs the benefits; and
- **Standards** – Standards bodies have been slow to reach a global consensus.

For mobile handsets, smart antenna deployment would be complex and expensive. For wireless Local Area Network (LAN) applications where the size, power and processing complexity constraints are relaxed, access points with smart antennas have a strong case and early versions are now available on the market. In mobile communications systems such as WiMAX smart antennas are already applied and will be applied further in commercial systems such as LTE. A semi-smart approach – where the communications signal from an antenna is broadened to a sector rather than a narrow beam is simpler and cheaper to introduce.

7.6 MULTIPLE INPUT – MULTIPLE OUTPUT (MIMO) SYSTEMS

MIMO systems use multiple antennas to increase the data capacity of a wireless channel making use of multi-path propagation which commonly occurs in urban environments. A data-stream is split into two or more smaller streams, each of which is radiated through a separate antenna. Multiple data-streams are transmitted through the same channel that would ordinarily be used for just a single data-stream. Signals from each of the spatially separated transmitter antennas follow multiple routes, termed multi-path, to the receiving antennas where they are recombined using complex processing to form the full capacity data-stream. The success of the increased data capacity of a MIMO system is dependent on a minimum spatial separation of the antennas relative to the radio wavelength used. Thus there are practical difficulties with small platforms such as mobile handsets and the use of lower radio frequencies (approx. 500 MHz and below). As frequencies of approximately 400 MHz have shown favourable performance in urban environments, the use at this frequency is restricted to a limited number of antennas per site. Furthermore, the data capacity of MIMO systems is dependent on the diversity of signal arrival angles and sufficient signal-to-noise ratio. In turn, these aspects are highly dependant on the (current) positions of radios in the physical environment. Research on this topic is ongoing. If MIMO systems will be deployed in UOs, it is likely to be in an asymmetrical form (MISO: Multiple Input – Single Output) where base stations and vehicle mounted systems have multiple antennas available for MIMO whereas the handheld units may have only a single antenna.

If the signal-to-noise ratio is not sufficient to increase the transmission capacity, adequate signal processing could result in an enhanced end-to-end quality/robustness instead of capacity enhancement. In this case antenna diversity processing applies rather than special multiplexing processing. The system should do an automatic selection of the processing approach. We could thus speak of adaptive MIMO. In the specific case of a persistent jammer, MIMO's multiple antenna configuration could be used to null

out the signal coming from the jammer's direction as another way of processing the antenna signals. In this case, smart antenna function is performed to continue communications at reduced data rate however at the penalty of reduced MIMO-performance.

MIMO used on-the-move is still in the research phase. The challenge is that the channel will change more rapidly than in static situations, requiring alternative processing and/or high processing speeds which will cause temperature problems. This may be used with and without feedback channels between receiver and transmitter. Today's systems offer MIMO on IEEE802.11n and advanced mobile systems. The advantages of MIMO in the current systems have not yet been operationally verified beyond the well known diversity schemes. Further, it is uncertain that feedback channels can be implemented in operational systems due to the fast changing channel properties and the difficulties of channel parameters estimation.

7.7 RELIABLE COMMUNICATIONS SYSTEMS AT FREQUENCIES ABOVE 60 GHz

The military demand for spectrum in the highly congested lower frequency spectrum bands means that there is now a need to consider the higher frequencies for communications systems. If greater use of the bands above 60 GHz could be made then this would provide a useful increase in the spectrum available for new services. These systems suffer much greater propagation losses making them unsuitable for long range applications.

These signals are highly reflective and this can be useful in urban environment but for only short range communications. Research has shown however, that the higher frequency bands could be useful for a range of applications, including:

- Broadband Fixed Wireless Access with very high capacities. This could allow large data applications such as video to be deployed on demand.
- Fixed line-of-sight point-to-point links, where link lengths of up to 5 km are envisioned with 99.99% availability, supporting short range backhaul.
- High speed (1 GB/s) short range wireless LANs, operating over a range of a few hundred meters. This could be used to provide access systems for large HQ's within buildings of opportunity such as large halls (e.g. HQs in factory buildings).
- Short range repeaters (500 m to 1 km) with very high data rates of up to 5 Gbps for applications such as HQ network interfacing.

7.8 LIMITATIONS IN AVAILABLE TACTICAL SYSTEMS

7.8.1 BOWMAN – Radio Limitations for Urban Operations

This section is a brief summary of work done to characterize the performance of operational systems in urban environments and the lessons learned. A complete report on the topic is included in Annex C of this report.

Users of Bowman Very High Frequency (VHF) Combat Net Radio are frequently unable to communicate with one another in urban environments due to poor radio frequency coverage. In order to maintain communications between personnel and HQ, manual (verbal) relay is required. This results in an increased need for equipment and puts personnel at significantly greater risk.

To quantify the extent of this problem, a commercial path loss prediction algorithm has been used to examine propagation in urban areas. The results are consistent with user observations that VHF

communications in urban areas are highly variable and with measurements as, e.g. reported in [22]. Propagation along streets could allow a communications range of several kilometres between users, whereas penetration into built up areas might limit the range to 200 meters or less.

Communications coverage could be increased by deploying relay stations, ideally located above ground level, for example on top of a tall building. However, the station may need to be manned in order to minimize the risk of theft or destruction. Airborne deployment is considered. Other potential solutions include the use of a propagation tool to quantify the extent of the problem prior to deployment, deployment of an expendable unattended relay, exploitation of any existing mobile phone infrastructure and the employment of Bowman High Capacity Data Radio (HCDR) to provide Voice over Internet Protocol (VoIP). It is noted that any solution should ideally be organic to the users and provide both a reliable and persistent capability.

The report recommended that:

- Lightweight expendable relays are developed;
- The use of airborne platforms, including manned aircraft, unmanned air vehicles and tethered aerostats is considered;
- The manufacturers be approached regarding additional functionality in the Bowman VHF radio to provide, in effect, two frequency simplex operation, automatic selection of a rebroadcast station (rebro), and export of a pressel signal;
- The development of a radio planning tool and a spectrum survey tool is considered;
- The use of HCDR to form a backbone communications network, using Voice over IP (VoIP) techniques be investigated; and
- The procurement of a secure Personal Role Radio is considered and that the waveform of this radio should be suitable for direct relay over longer links.

More information is being sought regarding the frequency choice and communication modes employed in practice, to see whether any guidelines can be developed. While there is doubt regarding the effect of these measures, it does offer a potential quick win if effective.

7.8.2 TETRA

TETRA is a European standard private mobile radio (PMR) system. TETRA systems are available as COTS equipment and networks are currently being installed around the world, used by military, public safety units and companies. TETRA offers the option of a relatively inexpensive spectrally efficient modern digital communications system with a number of features of particular interest to military users based on its target user base of professional PMR users, including public safety users who have participated in the development of the TETRA standards. The present and considerable installed base at both military and non-military organizations makes TETRA an obvious candidate for enabling wireless communications with local government, emergency response organizations, NGOs, etc., e.g. in CIMIC-operations. Another advantage of TETRA is that its radio frequencies near 400 MHz are favorable in physical urban environments, i.e. will yield the best mobile coverage. TETRA features both a cellular mode (Trunked Mode Operation) and a combat net radio mode (Direct Mode Operation). It should be noted however, that DMO has a sever range restriction if both handhelds are operated at man height. TETRA offers a DMO-TMO gateway function. With some restrictions, range extension may be possible using TETRA repeaters. TETRA does not feature TRANSEC but offers COMSEC of high quality.

7.9 COMMAND AND CONTROL CHALLENGES IN URBAN OPERATIONS

IST-046/RTG-008 was formed in the spring of 2004 to look at Command and Control Challenges in Urban Operations. They looked at how command and control processes in urban operations can be improved by emerging information technologies. The group developed information requirements at the battalion level and below. They also identified technologies that are currently available and the anticipated future developments that will contribute to meeting those requirements.

IST-046 focused on the echelons at battalion level and below, primarily because it was felt that there are numerous efforts and studies focused on higher echelons and because operations in urban environments are largely conducted at the lower echelons. The report provides a sampling of technologies and programs that have application in the urban environment. Generic technologies were identified to address information requirements related to specific urban needs. In most cases communications requirements were included in the information requirements. The group concluded that "*communications constitute a critical integration issue and greatly impact the system of systems approach addressed throughout the report.*"

Communications is a necessary component of any successful system of systems in Command and Control. The group's report says that "*communications are of critical importance to the entire system*". Some of the communications challenges identified by IST-046 are:

- No stationary communications infrastructure;
- High density of nodes and users;
- Security;
- Anti-jamming;
- Mobile routing;
- RF propagation and multi-path;
- Spectrum contention;
- High bandwidth applications (real-time video, etc.); and
- Network management in mobile, urban environments.

While the communications challenges just listed are not unique to the urban environment, the urban environment adds a degree of difficulty to each. Solutions to communications issues that work in lightly populated, simple terrain will not work in the complex terrain of a heavily populated urban area.

Command and Control can't function without adequate, reliable and secure communications. When the battlespace is in an urban environment the requirements for communication become more difficult and more critical to provide to the soldier. In an open battlespace where a vehicle is the primary entity, communications is less complicated. In an urban battlespace the individual dismounted soldier becomes the focal point of operations. Providing adequate access to communication resources is essential to the successful completion of the urban mission.

7.10 SENSORS FOR URBAN OPERATIONS

The majority of sensors will require significant communications in the urban area. While some urban sensors plan to use pre-processing or other communications reduction techniques, there is a realization that communications in the urban region will be complex and not have unlimited availability. Sensors located

in the squad or platoon tend to provide data to the soldier that is part of the system. While the communications to the soldier might be simplified because of distances it is complicated by power availability, increased desire for wireless communications, and the requirement to share the sensor data with others. If all the sensors were vehicle mounted or only designed for one user the problems would be greatly reduced. The use of sensors in the open is better defined and supported. When the soldier moves into buildings the capabilities become limited and are almost non-existent in underground environments. In this case moving to post-conflict operations does little to help the soldier. Sensors and their related communications at the soldier or platoon level are impacted significantly by the urban environment.

SET-076/RTG-044 “Sensors for Urban Operations” was formed in the fall of 2004 and conducted sensor demonstrations in 2006. They looked at what types of sensors were most useful in an urban operation context and to recommend research areas. The report provided 42 detailed descriptions of sensor technologies that could be deployed in urban operations. The descriptions include how the sensor would be used, system specifications, a technology descriptions, and in most case communications requirements. Of the sheets that do provide a communications requirement five (5) require high bandwidth communications to stream imagery. Another six (6) require a radio or standard data link to transmit data. One (1) sensor plans to do pre-processing to limit communications and will only have to transmit a single image frame instead of a stream of images. This is an example of trading off processing power at the sensor for reduced communications bandwidth use. A review of the thirty (30) data sheets without specific statements about the communications requirements provides the following insights. An additional three (3) sensors seem to need high bandwidth communications to stream imagery. A radio or data link is needed by twelve (12) of the sensors. The remaining sensors seem to be designed to be placed on the soldier, a vehicle, or a fixed position like a checkpoint. This last group will be directly linked to the user and minimize the need for communications.

SET-153 “Multi-Sensors Integration for Urban Operations” began in 2009 to continue the examination of sensors in urban environments.

7.11 OTHER RELATED PROJECTS

Although our workgroup did not examine them, several other communications related test and evaluation programs are ongoing at several NATO and EDA member national labs that could contribute to near-term improvements in tactical communication in urban operations:

- Contributions within the European Defence Agency (EDA)-project WOLF (Wireless Robust Link for Urban Force Operations) under the Defence R&T Joint Investment Programme on Force Protection A-0120-RT-GC [28].
- High altitude platform communication relay tests in the Netherlands: “*High Altitude Radio Relay Measurements*” [23].
- DARPA XG (USA).
- DARPA Disruptive tolerant network (USA).
- DARPA Wireless network after next (USA).
- Frequency Evaluation Tests (Canada and Netherlands).
- MANET Experiments (Germany).
- WiMAX Tests (Germany/Italy).

Chapter 8 – NATO NETWORK CENTRIC WARFARE CONCEPTS COLLIDE WITH TACTICAL OPERATIONS IN URBAN ENVIRONMENTS

NATO and its member nations have embarked on research, development and modernization agendas to capitalize on the promise of modern information processing and dissemination technologies in what is known as Network Centric Warfare (NCW). Network-centric military operations are operations enabled by networking military forces and sensors to provide an integrated picture of the battlefield, available in detail at all levels, down to the individual soldier. This extensive information sharing and synchronization is to be achieved by equipping command posts, vehicles, and individual soldiers with GPS, computers, and displays, all linked by wireless, radio-frequency networks. Annex D of this report is an example of a National NCW focused modernization plan, provided by Italy.

NCW capabilities are said to include:

- Self-synchronization – warfighters doing what needs to be done without traditional orders.
- Improved understanding of higher command's intent.
- Improved understanding of the operational situation at all levels of command.
- Increased ability to tap into the collective knowledge of NATO and coalition forces to reduce the "fog and friction" of war.

The *Theory/Assumption* of NCW is that combat power is increasingly derived from information sharing, information access, and speed. The perceived advantages of NCW include:

- Networked forces can consist of smaller units traveling lighter and faster. Fewer troops, with fewer platforms, and fewer supplies can perform a mission effectively, or differently, at lower cost.
- It is harder for an enemy to effectively attack a widely dispersed formation.
- Units can cover much more ground, because they do not have to maintain a formation or slow down for lagging vehicles.
- Knowing the location of all friendly units reduces fratricide during combat operations.
- 'Swarming' tactics allow an attack to be directed straight into the heart of an enemy command structure, undermining the enemy from the inside, rather than battling only on the periphery.

The center piece of NCW is improved Situational Awareness (SA). SA is:

- Knowing where you are with accuracy (self location) – based on the Global Positioning System (GPS).
- Knowing where your friends are – based on automated exchange of GPS information.
- Knowing where the enemy is – based on rapid and synchronized collection and timely dissemination of intelligence.
- All displayed as icons on digital maps, in near real-time, on rugged computer displays.
- SA is the center piece of the goal of a 'Common Operational Picture' (COP).
- A shared COP is the center piece of NCW.

Annex D of this report provides detailed descriptions of the architecture NATO has devised for implementing NCW and one nation's plans and programs for modernizing to that standard. The focus of

this report has been on the difficulties modern communications systems face in urban environments. Current systems are extremely stressed in attempting to deliver the promise of NCW in best case conditions. Urban environments are far from ideal conditions and current communications will not adequately support the NCW concept in urban environments. New technical approaches and systems briefly discussed in Chapter 7 of this report hold considerable promise for improving the performance of communications systems in urban operations, but as we state in this report's conclusion, they will not deliver on that promise without a much more concerted effort to harness their power in direct support of the urban operations communications challenge. Without adequate communications systems, NCW concepts cannot be executed and current and near term communications systems will not adequately function in anticipated urban operations environments. Much more needs to be done.

Chapter 9 – SUMMARY AND CONCLUSIONS

Communication in and between the multiple dimensions of urban environments is an extremely difficult technology challenge. Urban structures, materials, object densities and configurations (such as urban canyons), interference from a large diversity of electronic devices and power constraints associated with man-portable radios significantly degrade wireless communications. This causes problems at brigade-level and below where commanders rely heavily on constant wireless/radio contact with subordinates.

9.1 SUMMARY

Tactical communication problems may disrupt the ability to maintain a common operational picture (COP), to give orders and guidance, to request support, or to coordinate and synchronize units. In other words, tactical communication problems in urban areas can basically derail network centric operations. Establishing and maintaining high priority command communications links will take concerted effort and resources, and may dictate tactical plans.

Current systems and short-term technology improvements cannot overcome the communication challenges of urban operations, but proper tactics, techniques, and procedures (TTP) based on lessons learned from ongoing urban operations can significantly improve communications in these environments. These TTP and lessons learned include:

- Extensive use of retransmission and relay sites/equipment. This may include unmanned aircraft, aerostats and possibly also blimps. Such platforms could provide ISTAR capability and communications relay payloads. In particular, in the future it may also accommodate a Dynamic Frequency Assignment module for cognitive radio.
- Use of non-terrestrial capabilities such as satellite communications systems.
- Use of wire lines.
- Airborne command posts.
- Careful positioning of commanders, command posts, and antennas to take advantage of urban terrain characteristics.
- Improvisation such as using visual signals and markers.
- Detailed communications analysis for movement planning to avoid dead zones and interference between units.
- Increase use of local civilian infrastructure.
- Messengers.

Some very promising technologies on the mid-term and long-term horizons have the potential to make major impacts on the challenges of urban communication:

- Software defined radio (SDR), offering, e.g. increased interoperability.
- Cognitive radio, offering enhanced radio link flexibility in, e.g. urban environments.
- Multiple Input, Multiple Output (MIMO) technology. Adaptive MIMO may offer significant increases in data throughput or link quality without additional bandwidth consumption or transmit power.
- Smart antennas (in combination with MIMO) to enable range extension, reduction of interference and nulling out persistent jammers.

- Mobile ad-hoc network (MANET) radios. Some MANET capable radios, such as the Raytheon MicroLight, have recently become available.
- Terrestrial trunked radio (TETRA), offering multiple advantages for use in UOs.
- Ultra-wide band radios.
- Advanced commercial mobile communications approaches.

9.2 CONCLUSIONS

The IST-067 workgroup recognizes the limitations of this report. This report is an overview of possible approaches to solving communications problems, rather than a detailed plan. On the other hand, we feel strongly that there is important information in this report for many elements of the NATO community. Our group had an appropriate mix of nations and skills – academic, industry, and military. As a result, there are lessons in this report for military personnel on the complexities of communicating in urban environments and which technologies may solve some of their tactical communications issues. There are lessons for the industry and research communities that should help them understand the tactical-urban environment so that they can better focus their research and experimentation.

None of the approaches in Table 9-1 below is a “one size fits all” solution for tactical communications in urban environments. Each approach has strengths and weaknesses. It will require the synergistic combination of the results from several of these approaches to fully allow the implementation of NATO NEC in urban operations. Future systems must be able to adapt rapidly to the unpredictable complex urban environment as much as possible and as autonomously as possible. This implies constant compromises by autonomously selecting the proper modes of operation (i.e. selecting frequency, modulation, terrestrial or communications via air platform, interference and jammer suppression vs. throughput, the proper signal processing techniques). This report describes some enabling technologies that in time may solve these communications issues.

Table 9-1: Summary of Promising Technologies that Have the Potential to Make Major Impacts on Tactical Communication in Urban Operations (their horizons are indicated in different colors: Green = near-term; Yellow = mid-term; Red = long-term)

Technology	Description	Opportunities for Urban Operations	Challenges
IEEE802.16 d/e/j WiMAX	Base-station dependent mobile (e) or stationary (d) wideband terminals. Relay functionality to overcome NLOS-problems (j).	COTS equipment. 802.16 j) may overcome some of the NLOS problems.	Infrastructure-based. Obstructions of LOS make d) and e) less suited for UOs.
MANET	Mobile ad-hoc networks.	Ad-hoc protocols adapt to the dynamic behaviour of the links in the urban environment.	Lack of COTS communication nodes. Routing, autonomy, and robustness.
Heterogeneous MANET	Advanced Mobile ad-hoc networks.	Likely with airborne component(s).	Dealing with links of different natures. Routing, autonomy, and robustness.
IEEE802.22 Cognitive Radio	WiMAX-like services primarily for rural areas in vacant TV-bands.	Intelligence in the radio nodes will ease provision of frequencies and adaptation to changing propagation conditions. COTS like eq. with WiMAX features.	Same as for WiMAX. See above.
Software Defined Radio	Portable waveforms deployed on generic radio hardware.	Interoperability. Re-use of HW and portability of waveforms. Likely enabler for cognitive radio, especially in the mid-term future.	Price, size and power consumption of equipment.
Dynamic Frequency Broker	Automatic frequency assignment, intelligence gathering.	Intelligence and surveillance gathering made easy. More efficient use of spectrum.	Standardization. Vulnerabilities of single-point failure of the broker.
On-the-Move and Adaptive MIMO-Smart Antennas	Multiple antennas to exploit multi-path propagation and mitigate interference and jamming effects.	Increased capacity (diversity gain), pre-compensation, or increased link robustness and less interference.	Larger antenna arrays and price. Theoretical; remains to be proven. Rapid and accurate feedback information needed.

Ongoing work at NATO member national labs, and the longer term technology advances listed above have the potential to improve tactical communications in urban environments, and while proper TTPs based on lessons learned from ongoing urban operations can significantly improve communications in these environments, the bottom line is that current technology and systems are NOT adequate to support fully integrated NCW operations (not robust enough for military use) in urban environments.

Real-world combat operations are NOT where we want to do our testing. The true usefulness, applicability, and value of the TTPs, approaches, and technologies available will never be fully understood unless they are operationally tested and evaluated in an integrated and fully instrumented urban operations test site. This test facility must include all the dimensions of the true urban environment: underground tunnels, complex street layouts; and large/deep high rise structures. The efforts and technologies listed above represent potential improvements, but much more focused research and development on how they are applicable to the challenges of communicating in/between all the dimensions of the urban environments is needed. NATO members and the NATO Research and Technology Organization members should push for the funding and execution of research and development programs that are directly focused on tactical communications for urban operations.

Chapter 10 – REFERENCES

[1] U.S. Army: *Field Manual 3-06 Urban Operations,* Department of the Army, October 2006, pp. 2-4.

[2] Neuman, W., *Police Won't Use $140 Million Radio System,* New York Times, January 25, 2007. http://www.nytimes.com/2007/01/25/nyregion/25radio.html?_r=1&scp=1&sq=where%20signals%20mix%20police%20communication&st=cse&oref=slogin.

[3] *Urban Operations in the Year 2020,* RTO-TR-071, AC/323(SAS-030)TP/35.

[4] *Doctrine for Joint Urban Operations,* Joint Publication (JP) 3-06, 16 September 2002.

[5] *Joint Communications System,* Joint Publication 6-0, 20 March 2006.

[6] Boysen, E.S. and Kjuus, H.E., *Proactive Handover using SIP,* NATO IST-083/RSY-018 Symposium on Military Communications with a special focus on Tactical Communications for Network Centric Operations, Prague, 21-22 April 2008.

[7] Overduin, R., *A Cellular-Based Solution for Radio Communications in MOUT,* MILCOM2005 Proceedings.

[8] Handbook for UO: JP 3-07, *Joint Doctrine for Military Operations Other Than War,* 16 June 1995.

[9] Schwartz, Maj. Gen. N.A., USAF, *The Role of Aerospace Power in Joint Urban Operations* www.rand.org/pubs/conf_proceedings/CFI48/CF148.appc.pdf.

[10] Delmee, M.H.M., Voogd, J.M. and Verkoeijen, P.C.F.M., *Vignettes Unmanned Systems* TNO-DV 2006 A238 (in Dutch), The Hague, Netherlands, August 2006.

[11] Overduin, R., *Trials on Mobile Communication in Military Urban Terrain,* TNO Report Nr. 34205 (in Dutch), Delft, Netherlands, December 2006.

[12] Street, M.D. and Szczucki, F., *Wireless Communications Architecture (Land): Scenarios, Requirements and Operational View (NATO Restricted) NC3A Technical Note 1246,* The Hague, Netherlands, December 2006.

[13] *Critical Information Requirements Table,* Command Center Challenges for Urban Operations IST-046/RTG-018.

[14] *Patrol in Lamuk Valley,* SMP Research Program V205 Brochure (in Dutch) TNO, December 2006.

[15] *Demonstration of Sniper and Gunfire Detection Systems,* Aberdeen Proving Grounds, 2006.

[16] *Policy on the Use and Management of the Radio Frequency Spectrum,* (NATO Unclassified) AC/322-D(2006)0020-REV1.

[17] *NATO,* AC/322(SC/3)D(2007)0003-Rev4 SMADEF XML Documentation Release 1.2.2 03 July 2008, http://www.smadef.net/122/smadef_20080703.pdf.

[18] Report from the NATO SMB- Serge Basso. February 2006, Bristol NC3B/ SC/6 AHWG/2 Meeting, and Paris September 2006 Meeting.

[19] *Minimum Operational Performance Specification for Airborne VHF Receiver-Transmitter Operating in the Frequency Range 117.975-137.000 MHz,* EUROCAE ED-23B, March 1995.

[20] CCEB Spectrum Task Force: *Net-Centric Spectrum Management and Operations Review (final),* October 2007.

[21] Maseng, T. and Ulversøy, T., *Dynamic Frequency Broker and Cognitive Radio,* Submitted to IEEE Communications Magazine, 28 August 2007.

[22] Feenstra, P., Overduin, R. and Trommelen, P.H., *Indication of the FM9000 Performance in Urban Operations,* (in Dutch) (Indicatie van de prestatie van de FM9000 in Optreden Verstedelijkt Gebied) December 2004, TNO Report 33320.

[23] Overduin, R. and Rijsdijk, P.J.M., *High Altitude Radio Relay Measurements,* TNO White Paper, October 2008.

[24] IST-035/RTG-015, Final Report: *Awareness of Emerging Wireless Technologies: Ad-Hoc and Personal Area Networks, Standards and Emerging Technologies,* April 2007.

[25] IEEE Standards Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, NY, 1990.

[26] United States Government Accountability Office: *GAO Highlights, Highlights from GAO-08-877,* April 2008.

[27] Ulversøy, T., *Software Defined Radio: Challenges and Opportunities,* Submitted to IEEE Communications Surveys & Tutorials, April 2008.

[28] European Defence Agency: Contract A-0692-RT-GC *"WOLF", Wireless Robust Link for Urban Force Operations,* http://www.eda.europa.eu/genericitem.aspx?id=370.

[29] Oostveen, J. and Overduin, R., *Perspectives of Multiple Input-Multiple Output (MIMO) Technology for Military Operations,* TNO White Paper, October 2008.

Annex A – TNO WHITE PAPER 34626 ON "CONSEQUENCES OF THE CELLULAR CONCEPT IN URBAN OPS AND REALIZATION PERSPECTIVES"

TNO Information and Communication Technology

Brassersplein 2
P.O. Box 5050
2600 GB Delft
The Netherlands

T +31 15 285 70 00
F +31 15 285 70 57
info-ict@tno.nl

TNO white paper 34626

Consequences of the cellular concept in Urban Ops and realization perspectives

Date	28 December 2007
Author(s)	R. Overduin
Number of pages	19
Number of appendices	-
Customer	Royal Netherlands Army (RNLA)
Projectname	Transmission Systems in Urban Operations
Projectnumber	035.31542

Contents

Glossary

3GPP	Third Generation Communications Partnership Project
BMS	Battlefield Management System
C2SC	Command & Control Support Centre
CIS	Communication & Information Systems
CNR	Combat Net Radio
COP	Common Operational Picture
COST	European Co-operation on Scientific and Technical Research
DCMO	Data Communication in the Mobile Environment
EPM	Electromagnetic Protection Measures
ESM	Electromagnetic Support Measures
GBSA	Geographically Based Situational Awareness
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
MDNA	Mobile Domain Network Architecture
MIMO	Multiple Input Multiple Output
NBS	Networked Battle Space
PC	Platoon Commander
PR4G	Poste Radio 4eme Generation
RF	Radio Frequency
RNLA	Royal Netherlands Army
SIMO	Single Input Multiple Output
TC	Team Commander
TETRA	Terrestrial Trunked Radio
UAV	Unmanned Aerial Vehicle
UMTS	Universal Mobile Telecommunication System
VHF	Very High Frequency
VoIP	Voice-over-Internet Protocol

1 Introduction

Recent military missions have shown an increasing need for resilient radio connections in urban operations for obtaining situational awareness within relatively small units. Radio connections in urban environments suffer from object blocking and man-made noise. Both phenomena vary highly in time, also due to unit agility. Research [1][3] showed that the radio connection availability of RNLA's current CNR (Combat Net Radio), PR4G (Poste Radio 4eme Generation), is unreliable for radio connectivity between vehicles at the levels of platoon and team. Also, it has been concluded that a cost effective approach, answering the radio communication requirements at these levels in urban operations, is far from evident.

In 2005, the so-called cellular approach was introduced as an alternative urban operations telecommunication solution instead of current CNRs and possible future ad hoc networks [3]. Although military aspects and further technical implementation possibilities of this idea have been discussed, not all have been quantitatively addressed. However, the requirement for quantification and further analysis of this approach emerged, especially for the Netherlands Urban Operations missions. In accordance, this resulted in an assignment to TNO ICT and finally in this white paper.
The communication within a squad has not been considered in this assignment to prevent interference with other, current Defence projects focusing on the communication with and within squad level. This study will consider radio communication in the high mobile domain in a built-up urban environment at the level of platoon and team vehicles. This reflects a worst case for radio communications since it yields many challenging factors for radio communications: outside of severe signal blocking and the presence of man made noise mutual distances (and hence coverage) may vary considerably and rapidly.

One major disadvantage of the cellular approach that remained (both qualitatively and quantitatively) unsolved is that of lack of EPM (Electromagnetic Protection Measures). Thus, in this study not only the operational, organizational and practical consequences of several implementation alternatives have been considered but first of all the perspectives to add in certain extend EPM capabilities (other communication security aspects may be subject to future research). To quantify these perspectives, a reference scenario has been identified together with the RNLA, which will be discussed in Chapter 3.
Firstly, the implementation alternatives which are used throughout this study followed from a resume of previous, recent TNO research (Chapter 2) will be resumed. In Chapter 4, the several consequences of applying these alternatives will be discussed in the fields mentioned above, starting with a discussion on EPM aspects (in conjunction with attaining coverage) in the reference scenario. Boundary conditions will be identified and possible solutions will be suggested in this chapter. In conclusion of this chapter the organizational and practical consequences of the cellular system approach under the boundary conditions imposed upon by coverage and certain EPM will be dealt with.
In Chapter 5, the relation with the current MDNA (Mobile Domain Network Architecture) of RNLA's C2SC/NBS (Command & Control Support Centre/Networked Battle Space) team will be dealt with. Chapter 6 gives a conclusion on the realization perspectives of the implementation alternatives envisaged.

2 The cellular approach: implementation alternatives

As shown in previous research for Netherlands Defence and the national trial in November 2006 [4], VoIP over GPRS (Voice-over-IP over General Packet Radio Service) did not proof to be operationally viable. The only way to make it principally work is to use GPRS for data only and use GSM for voice. If a common IP-interface is required, other approaches will be necessary to obtain an acceptable initiation delay, comparable with TETRA (Terrestrial Trunked Radio) delay values (i.e. maximally approx. 200 ms).

One major positive outcome of the November 2006 trial was that with the 900 MHz radio frequency (RF) a satisfying coverage in urban terrain could be achieved. Even in pre-assumed dead spots, there appeared to be sufficient coverage. This appeared the case since in the specific urban area commercial operators provided ample coverage. Therefore, there was no reason to apply GSM repeaters in this trial.

Hence, a mutual comparison of several cellular system alternatives within the 400 – 900 MHz band has been considered a logical next step. This means that GSM900 and TETRA (Release 1) may be considered as candidate systems. Theoretically, UMTS900 might also be considered as an option. However, the market penetration and hence the availability of UMTS900 systems is still very uncertain at the moment of the writing of this report. If UMTS900 systems would widely emerge its bandwidth performance is expected to be somewhat larger compared to that of GSM-systems at equivalent coverage.
Referring to the outcomes of the November 2006 trials, GPRS with GSM900 (i.e. non-common IP interface) has not been excluded as an option, albeit that a serious drawback of this solution is that some booby traps are designed to detonate on GSM/GPRS signals. The question is if it is practically feasible to countermeasure this. However, also for other cellular systems neutralization of such threat is a point of concern.

Initially, WiMax seemed also of possible interest. Advantages of WiMax are its higher bandwidth and therefore transmission capacity and the increased reflectivity to objects at approx. 3.5 GHz. However, its high radio frequency yields smaller cells and less penetration through objects as verified by measurements in e.g. the Netherlands, reporting ranges below 2 km.

3 Reference scenario

For this study, a vehicular satellite patrol scenario has been selected. This scenario has also been enrolled in the November 2006 Netherlands trial [4]. In Figure 1 a deployment is shown with example movements of a team/ company vehicle and two platoon vehicles.

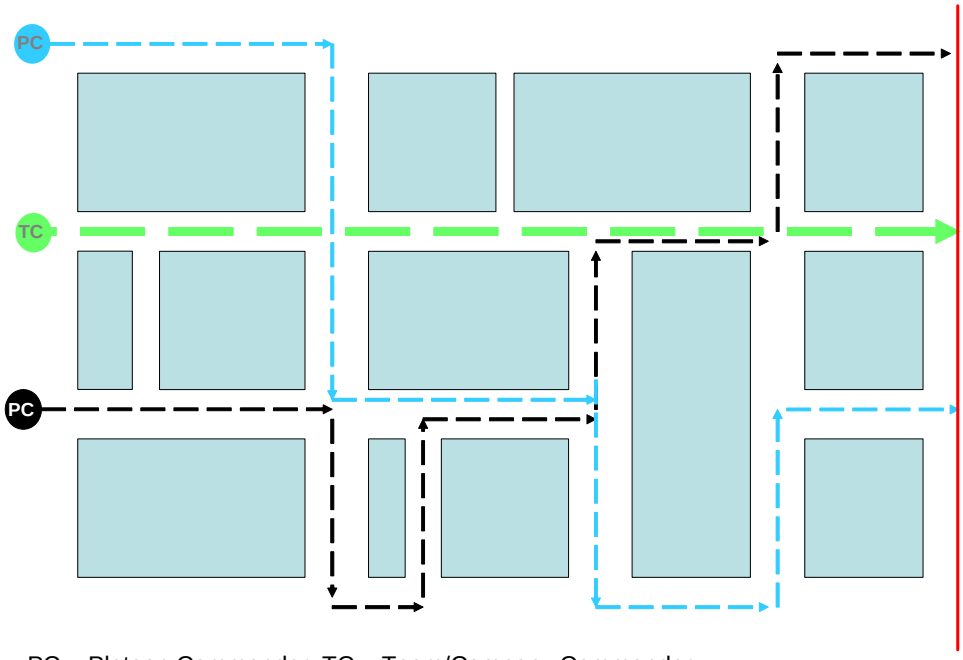


Figure 1: Vehicular satellite patrol example for one team vehicle and two platoon vehicles

The intention is that no unit will be substantially abreast of others. This means that vehicle movements, starting from the left, will take place fairly synchronized. This results in a more or less simultaneous arrival at the red target line depicted in Figure 1. From this target line, troops using combined arms will continue to achieve the final mission target, possibly implying object penetration.
It is assumed that the vehicle with the base station will be deployed at battalion level or at the level of the CIS team/ company and will move towards the edge of the hazardous urban environment where the actual urban operation will commence (Left in Figure 1). In this relatively safe area the base station vehicle will be at a semi-fixed location, where protection measures will be taken such as camouflage, protection by military personnel and redundancy (provided by back-up means).

In [1] it is stated that the mutual *maximum* distances between platoon and team/ company vehicles may be assumed to be approximately 2 km. This value is therefore used as ballpark value in this scenario for the communication distances between the vehicles.
A second value that is required is the maximum distance of the (vehicle-mounted) base station to the platoon and team vehicles. Based on an average size of an *uninterrupted* urban built-up area in the form of a ward or borough this distance will be approx. 8 km.

This distance results from interpretation of Metropolitan area data from four major cities in the world: Tokyo, Paris, London and New York City [5], which proved to be quite similar. As expected, in [7] for the Turin built-up area, smaller sizes (3.6 km x 6.5 km) have been mentioned.

For propagation characteristics, it is required to distinguish between built-up areas and the lower urban parts (see also Chapter 4). Obviously, the built-up areas are of prime concern since these environments will cause major blocking effects for relatively low (vehicle-mounted) base station antennas.

Note that communication during the troops displacement phase towards the edge-of-battle will normally not be provided by this means. This concerns patrol movements through areas with lower buildings in relatively broad avenues and streets. There communication may be obtained by use of SATCOM, HF or via alternative, future airborne platforms such as blimps, aerostats or UAVs (Unmanned Aerial Vehicles). RNLA's current DCMO/BMS (Data Communication in the Mobile Environment/ Battlefield Management System) project will take into consideration such long range communication means.

Note that indicative displacement distances through the suburbs for the four cities mentioned above will vary from 120 km (Tokyo) to 40 km (London) [8].

4 Applying the alternatives in the reference scenario

This chapter considers the technical, operational and organizational consequences of the 400 MHz and 900 MHz systems in the fields of EPM, coverage and other aspects such as required protection measures (physical, redundancy), training & education, maintenance, materiel overhead and logistics (required assets and transport of central components to and within an area-of-operation) and management & control will be qualitatively dealt with. A quantitative assessment of organizational issues and their cost implication is beyond the scope of this technical study.
Technical and operational aspects focus on the EPM- and coverage issue that will be dealt with more quantitatively, using the aforementioned reference scenario as a basis. Firstly, a more generic introduction into this subject applied to cellular systems is given.

4.1 EPM and coverage

As motivated in [3] there are no cost-effective possibilities to add a certain form of EPM in a cellular system air interface. The only way to provide some protection is by procedures (e.g. altering frequencies, selecting frequencies with respect to the enemy's frequencies, providing redundancy) or to realize a certain on-air protection by (statically or dynamically) controlling the radio coverage. This is realized by narrowing down the azimuth beamwidth of the base station antenna. This lowers the probability of detection if the threat is expected from the left, right, or behind. There will only be a signal increase for the illuminated area in front of the antenna, where own and hostile battle units are present. Since the base station is assumed to be truck-mounted and controlled by military, this provides possibilities for altering the antenna beam characteristics.
The effect of narrowing down the antenna beam is that not only the interception probability of an enemy outside of the main lobe is decreased but that also the communication range is somewhat increased.
In case the signal is nevertheless detected, there will be more radiated power required to cause a sufficient jamming-to-signal ratio to jam the system outside its antenna main lobe. However, this mitigation effect against jamming is expected of much less practical value.

4.1.1 Boundary conditions from the reference scenario

The condition for applying the above approach is that own units need to be in the main lobe at all times to ensure communication via the base station.
The first boundary condition for this is that the *base station antenna height* has to be sufficient to allow for communications within the reference scenario over the maximum range of 8 kilometers (for the given base station antenna azimuth and elevation beamwidths). This condition requires careful propagation modeling which will be dealt with in more detail separately at the end of this paragraph.

The second boundary condition is that the *azimuth base station antenna beamwidth* has to be adjusted within the reference scenario to cover all the vehicles at all times. This means that at the left hand (starting) line in Figure 2, the base station antenna should initially illuminate 180 degrees to cover vehicles starting to move to the right (target) line and that it should *in theory* illuminate 14 degrees if the vehicles have reached the (right hand) target line (see Figure 2).

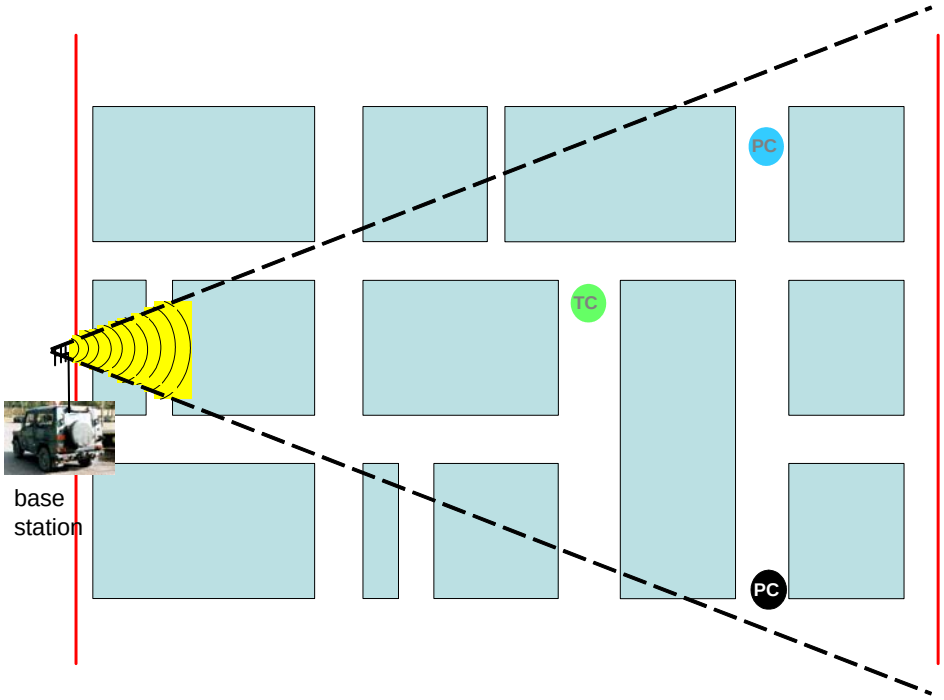


Figure 2: Azimuth illumination of the vehicular satellite patrol area by the base station antenna

Hence, a dynamic narrowing down of the antenna (e.g. in several steps) is required. From EPM point of view, it is desired to obtain a beam as narrow as possible. However, this implies the hazard of loosing coverage with a vehicle of the team. To enable the adaptation of beamwidth, current vehicle coordinates are assumed to be known at the base station. This can be realized by automatically (periodically) transmitting the vehicle positions to the base station.

Concepts and experiments with adaptive (smart) antennas for cellular systems are known [9][10][11], i.e. for 3G and 4G systems. Often such experiments take place in the framework of realizing mobile MIMO (Multiple Input Multiple Output) or mobile SIMO (Single Input Multiple Output). However, these indicate the feasibility for frequencies above 1 GHz. The use of smart antennas for as low as 400 MHz is also thinkable, however not evident since dimensions (i.e. antenna element spacings) become accordingly larger.

A major problem is that *in reality* the contours of the beam illumination on the ground (so-called footprints) will be unpredictably deformed by the urban objects, even if illumination takes place from high altitudes. The COST-231 Extended Hata model [12] indicates the *statistics* of this deformation in the form of a path loss standard deviation from the total path loss for a given distance between base station and mobile.

The variation in path loss is described by the log-normal distribution term (commonly used to describe slow fading or shadowing). Elementary statistics yield that 68% of the path loss values are to be expected within the interval of positive minus negative standard deviation around the mean path loss value (see Figure 3).

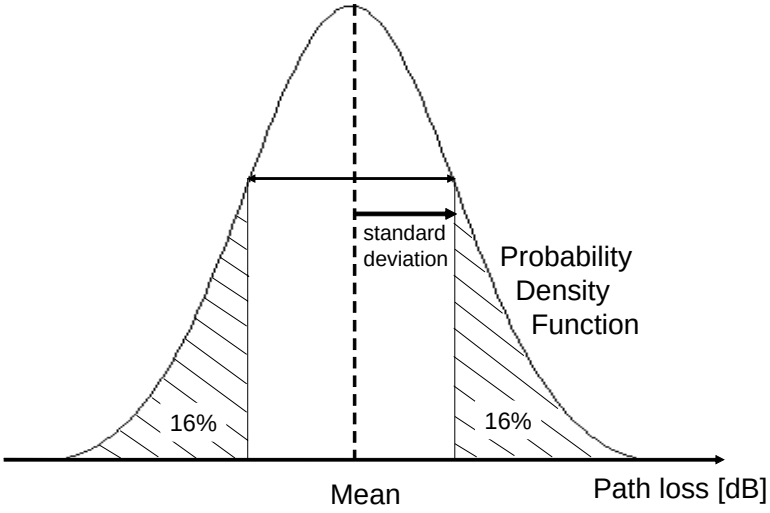


Figure 3: Path loss probability density function with 68% probability interval

This deviation measure may be assumed to calculate the worst case link budget. The Extended Hata model reports a 9 dB standard deviation value in urban terrain for distances larger than 600 m, independent of frequency and antenna heights. This value will be taken as a required link margin.

Because of the unpredictability of the footprint, antenna beam adjustment will require that not only vehicle positions but also signal quality has to be fed back to the base station transmitter that has to adjust its beamwidth accordingly. Care should be taken to realize a stable system with an acceptable adjustment rate.
Beamwidth adjustment can be realized coherently by altering the transmitter power to each individual antenna element of a transmitter array of e.g. four antennas. At the receiver side, separate antennas could be used to do the beam forming using baseband information and combining individual signals using processing software.

Finally, the third boundary condition forms the *elevation base station antenna beamwidth*. Like with the azimuth footprint, the elevation beamwidth will narrow down as the vehicles approach the target line. The value of the elevation beamwidth determines the current elevation footprint for a given effective antenna height and current distance. The desired minimum footprint size is dictated by the maximum mutual platoon vehicle distance. This is assumed to be 2 km as stated in Chapter 3. Assuming a margin of 1 km to count for the -3 dB beamwidth points, we arrive at a 3 km elevation footprint.
Figure 4 denotes the relation between the functional parameters for the maximum distance (maximum base station antenna gain).

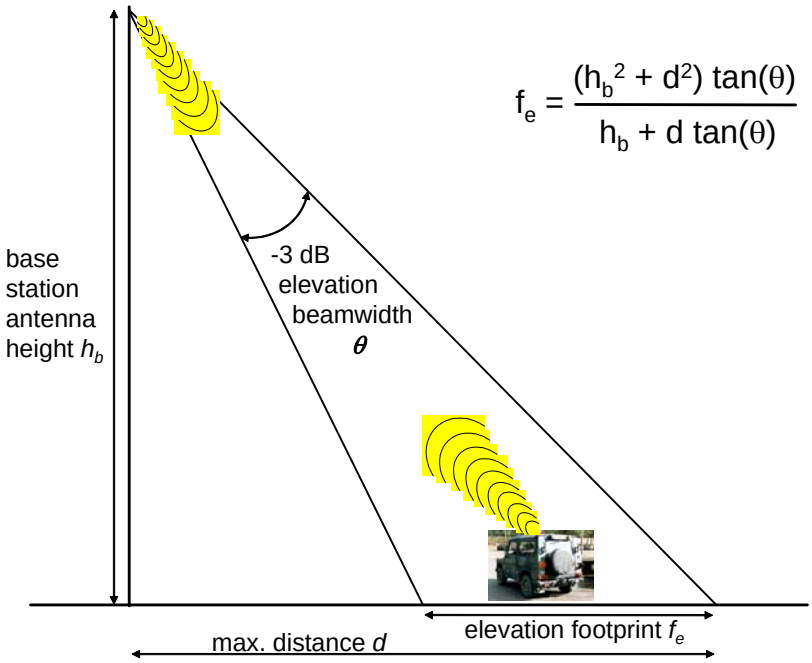


Figure 4: Elevation illumination of the vehicular satellite patrol area by the base station antenna

It will be analyzed in the next paragraphs for 400 and 900 MHz cellular systems which combination of beamwidths (i.e. EPM) and coverage is practically feasible for the reference scenario discussed in Chapter 3.

4.1.2 Propagation modeling

The analysis has been done using the Extended Hata model [12] that is generally accepted as empirical propagation model for mobile systems and therefore widely used. The interpretation of the several environment types this model uses, however, asks for careful interpretation.
The Extended Hata model uses the classification proposed and used in the basic Okumura model [12, p. 834]:

Urban:
Built-up city or large town crowded with large buildings and two-or-more-storied houses, or in a larger village closely interspersed with houses and thickly-grown tall trees.

Suburban:
Village or highway scattered with trees and houses - the area having some obstacles near the mobile radio car, but still not very congested.

Open:
No obstacles like tall trees or buildings in the propagation path and a plot of land which is cleared of anything 300 to 400 m ahead, as, for instance, farm-land, rice field, open fields, etc.

The above descriptions do not provide extensive quantitative descriptions of e.g. building densities (in % of the surface) and construction types. Some indication is given of the typical building height, but not for its statistics for a certain area type (suburban

or urban). This all complicates the interpretation of what each area is and hence, most important for this very study, as a consequence of the lack of height profiles, *how vast the several area types usually are, especially the built-up urban area*.
Some help is found in realizing that the area types are based on Japan, where building profiles in urban and suburban environments are much 'heavier' (large densities, great building heights) than in Europe or the USA [14]. Okumura's suburban area, for example, is to be interpreted as a residential metropolitan area in the USA (or Europe) with large groups of 'row' houses. Such is confirmed by a measurement campaign in the United Kingdom, concluding that Hata overestimates the path loss [15].
Finally, it has to be noted that the difference between urban and suburban areas increases with higher base station antennas. Truck-mounted base station heights are limited because of transportability. This somewhat limits differences between the propagation results for both urban and suburban area types.

From the above we may conclude that the Okumura urban area classification as also applied in the Hata model is to be interpreted as dense urban (business) center with large and high buildings and is usually (i.e. in an arbitrary urban operation) not larger than roughly 8 x 8 km as indicated in Chapter 3. A suburban area is a multitude vaster, very much depending on the actual city and will in general require use of separate long distance means.

The system range is determined by the uplink connection since the mobile terminal transmitter power is far below the base station transmitter power (the higher system sensitivity due to antenna diversity cannot fully compensate for this difference).

In the next paragraphs the quantitative analysis will be given.

4.2 GSM900/GPRS

In case of GSM900 the receiver system sensitivity is -98 dBm (6 dB above the 3GPP reference level), whereas the mobile transmitter power is 2 Watt (33 dBm). Furthermore, it is reasonable to assume a standard base station antenna gain of 14 dBi (90 degrees azimuth and 20 degrees elevation opening angles) [16].
The above means that the overall transmission attenuation that can be maximally allowed for proper RF signal reception is 145 dB for GSM900/GPRS. Assuming the link margin of 9 dB this results in a link budget of 136 dB.
Further assuming a base station height of 8 m and (conservatively) a mobile effective antenna height of 1.5 m, application of the aforementioned model yields a maximum range of approx. 870 m in urban environment and approx. 1.6 km in a suburban environment (in an open area a distance of approx. 5.7 km is attained).
Clearly, to answer operational acceptable range values in urban areas, a GSM900/GPRS system has to be enhanced with more directivity. It appears however, that practical possibilities to add more directivity to the base station antenna are limited to another 4 dB (yielding a total gain of 18 dBi and increasing the link budget to 140 dB). This only increases urban range with approx. 300 m and means that a relevant distance increase to reach the required 8 km can only be achieved by increasing the effective base station antenna height considerably.
In this configuration with enlarged directivity, the 8 km can only be achieved realizing an effective base station antenna height of 250 m. The attainable distance in a suburban environment in this case is 17 km, in open space 75 km.

A final decrease of antenna height can be obtained by applying a less usual sizing of the antenna to obtain considerable directivity in azimuth and elevation. Already, GSM panel antennas are encountered that yield 22 dBi gain (30 degrees azimuth and 7 degrees elevation beamwidth) [17], see Figure 5.

Figure 5: GSM high gain panel antenna

This yields a link budget of 144 dB. A base station antenna height of 175 m is now required for an 8 km built-up urban area distance. The distance will not increase in a suburban area and open space.

It can be proven that the theoretical elevation footprint in this case (110 m antenna height and 7 degrees elevation beamwidth is more than 7.5 km, which is more than sufficient to serve all vehicles.

4.3 TETRA (Release 1)

Mobile TETRA-equipment is designed to transmit at maximally 10 Watt (local regulation in the Netherlands allows for 1 Watt transmitter power). There will be a sufficient RF signal reception at -105 dBm. This difference with GSM base station receiver sensitivity is largely due to the fact that the bandwidth of TETRA Release 1 is approximately 8 times smaller than the bandwidth of GSM. In accordance, the overall transmission attenuation that can be maximally allowed for proper RF signal reception is 145 dB. Losses for diversity techniques and feeder losses add up to approximately 6 dB, resulting in 130 dB link budget, allowing for the 9 dB link margin. Assuming an 8 m effective base station antenna height, a transmitter height of 1.5 m and 400 MHz RF, this yields approx. 1.1 km maximum urban distance with the assumption that no directivity has been introduced as yet. In a suburban environment the maximum range is approx. 1.9 km (in an open area a distance of approx. 6 km is attained).
Adding practical realizable gain (i.e. 6 dBi for a regular sector antenna) brings the link budget to 136 dB. This results in an urban area distance of 1.6 km. The suburban area distance is 2.7 km and the open terrain distance is 8.5 km. The urban area distance of 1.6 km is still far from sufficient as there is still a large gap with the 8 km requirement.
In this configuration with enlarged directivity, the 8 km range can only be met with an effective base station antenna height of 140 m. The attainable distance in a suburban environment in this case is 14.5 km, in open space 54 km. Note that these last distances are lower than for GSM/GPRS.

Like with GSM panel antennas, in recent years TETRA panel antennas are manufactured that possess relatively high gains, large dimensions and weight however as a undesired consequence. As with GSM assuming a maximum acceptable panel length of approx. 2 m (and weight of approx. 30 kg), 17 dBi could be attainable [18], yielding 40 degrees azimuth and 19 degrees elevation antenna beamwidth. This

enlarges the link budget to 147 dB. For a 8 km built-up urban area distance, the effective base station antenna height now becomes 40 m. Like with the GSM base station antenna modification, the distance will not increase in a suburban area and open space (there even is a slight decrease).
The theoretical elevation footprint in this case (40 m antenna height and 19 degrees elevation beamwidth) is larger than 7 km, which is more than sufficient to serve all company vehicles.

The practical attainability of a 17 dBi antenna gain for TETRA compared with the 22 dBi gain feasibility for GSM the base station antenna indicates a difference of EPM of 5 dB in favor of GSM systems, assuming identical threat capabilities, i.e. ESM (Electromagnetic Support Measures) system sensitivity and jamming power at the base station at the corresponding frequencies. This difference is determined by the attainable gains for GSM and TETRA systems, respectively. Note that the EPM-benefit of this difference still applies if MIMO or SIMO would be introduced [19] (Figure 6). Moreover, due to the radio frequency, MIMO or SIMO would be more practically to implement in 900 MHz systems than in 400 MHz systems.

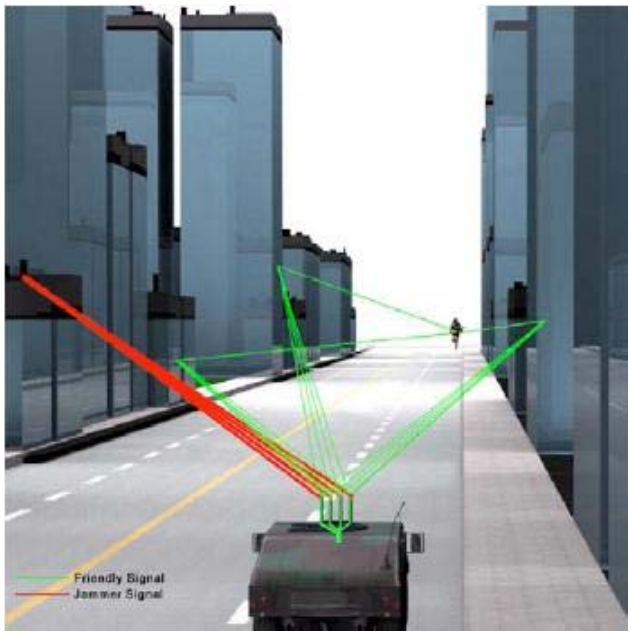


Figure 6: Impression of Mobile MIMO in a built-up urban area [19]

4.4 Organizational and practical aspects

There are several organizational and practical aspects associated with realization of the cellular approach analyzed in this chapter.

- It will take additional means in the sense of airborne platforms (UAVs, blimps or aerostats) to realize the required base station antenna heights. Also the weight of the antenna elements compels for airborne elements. Clearly this involves additional procurement, training, maintenance, truck-transportable launch platforms and preparation to setup and launch the system. The most critical point here is the proper selection of platform type depending on the

number of platoons to service and the area to cover, the desired level that is made responsible for the actual control of the airborne platform (team level or higher) and the stages where this platform will be active in (in built-up area only or also before that), et cetera;

- It is felt that using airborne platforms will take pre-mission planning efforts and during the mission adjustment of the coverage area of the platform. This means that current vehicle positions and movements will have to be known to the control level at any time;
- The above implies that there will be a necessity for dedicated and skilled airborne platform control personnel facilitated by a special unit for as many combat units as possible, i.e. added directly to a high organization unit (depending on the order of battle, e.g. battalion). However, if this is unit centrally manages the airborne platform and radio coverage properly, it will take away radio connectivity concerns at the combat units, providing concentration to their primary battle tasks.
- Protection measures will have to be taken in order to prevent a single point of failure. This applies to both the launch and control platform and the airborne platform. The required protection of the airborne platform is very much depending on the type, its altitude and the expected threat capabilities. In any case control asset redundancy will be recommendable.

Despite the considerable consequences mentioned above it is generally believed that airborne platforms are the most likely solutions to the tactical radio coverage problem in urban operations in built-up areas [21].

5 Coherence with C2SC's Technical Architecture for the Mobile Domain

In [20] several wireless communication/connection models are foreseen in the mobile domain at vehicle level. In two models the use of cellular systems is possible in:

1) The Hub-and-Spoke model (Figure 7, left);
2) A combined connectivity model in for instance a compound setting (Figure 7, right).

Specifically, GSM/GPRS/UMTS systems have been mentioned as examples for cellular systems. These however have not been further dealt with, i.e. advantages, drawbacks, transmission capacity and ranges, et cetera have been analyzed in a quantitative way. In this sense this TNO-study is complementary to [20].

Figure 7: Wireless connection models in which cellular systems could be implemented [20]. Hub-and-Spoke model (left) and combined connectivity model (right)

It is furthermore important to realize that the vehicular radio communications considered in this TNO-study is restricted to team (company) level and assumes the exchange of hierarchical information between the levels of team and platoon commanders but also between platoon commanders mutually for i.e. co-ordination purposes (all vehicle-based). Any possible exchange of Geographically Based Situational Awareness/ Common Operational Picture (GBSA/COP) information as referred to in [20] is handled, using the cellular systems, in principle within a single cell. Such information will be required for the adaptive antenna beamwidth as discussed in Paragraph 4.1.

In case a wider reach of the GBSA-information is required, there will probably (depending on how large the area is) have to be a separate arrangement for GBSA information exchange, resulting in a second radio per vehicle as suggested in [20]. However, in case aerostats, blimps or UAVs are applied to create effective base station antenna heights well above 200 m, the area footprint might well exceed to a vast suburban area, providing coverage at a battalion level. Depending on the sizing (cell coverage calculation, transmission capacity per user in the cell available for a certain total traffic load), such may offer perspective for processing GSBA information on a large scale.

In either case, the cellular approach will not conflict with the Technical Architecture for the Mobile Domain as this second radio will be dedicated to process only short GBSA messages with medium availability (an occasional miss of an update is considered acceptable).

6 Conclusions and recommendations

Comparison of the practical distances (i.e. distances of realistic system implementations) in urban areas with that of equivalent GSM systems demonstrates the advantage of TETRA over GSM900 systems as far as range and coverage in urban, built-up areas is concerned. This advantage in this area type is due to the difference of TETRA with GSM with respect to radio frequency.
The same difference however, yields more directivity for GSM systems than can be practically realized for TETRA systems. This results in an EPM that is approx. 5 dB larger than for TETRA systems, assuming identical threat capabilities at the corresponding frequencies. Addition of MIMO and SIMO enhancements to improve EPM threat resilience is more practically realizable for 900 MHz systems such as GSM/GPRS, consolidating the advantage with respect to EPM for these systems over 400 MHz systems.

Quantitative analysis shows that only substantial addition of base station antenna directivity (i.e. gain) substantially decreases effective antenna heights and may add a certain EPM by controlling the footprint, as was the prime goal of introducing base station antenna gain. However, even with gain enhancement techniques, considerable base station antenna heights result that in most cases will only be feasible with the use of airborne relay platforms such as aerostats, blimps or UAVs.
If required, range enhancement can be obtained if an airborne node is introduced. In this case, if the effective antenna height exceeds approx. 2 km, the size of the elevation footprint has to be checked not to become lower than the minimum elevation footprint operationally required.
In the case of airborne platforms, multiple small antenna beams or maybe one broader might cover a considerable suburban area as well. This might offer perspectives for integral GSBA message handling (i.e. at battalion level).
In general, airborne platforms are considered as the means to obtain coverage in difficult radio propagation areas such as urban environments. In this sense, the use of VHF CNR means in such airborne concept is not to be excluded, depending on the need for bandwidth, link quality and the number of units to be serviced [22]. The advantages of using VHF CNRs are the availability of current organizational means and of the CNR EPM capabilities.

The implications of using airborne platforms are that there will be a necessity for thorough mission pre-planning and a continuous situational awareness for all vehicles to be serviced. This requires dedicated and skilled airborne platform control personnel facilitated by a special unit for as many combat units as possible, i.e. added directly to a high organization unit. Besides of additional assets such as truck-transportable launch and control platforms this clearly involves education, training, maintenance and protection measures (e.g. control asset redundancy) in accordance.

7 References

[1] P. Feenstra, R. Overduin, P.H. Trommelen:
Indication of the FM9000 performance in Urban Operations (in Dutch)
(Indicatie van de prestatie van de FM9000 in Optreden Verstedelijkt Gebied)
December 2004, TNO report 33320

[2] J. Andrusenko:
Military Operations in Urban Terrain
MILCOM2004 Proceedings

[3] R. Overduin:
A Cellular-based Solution for Radio Communications in MOUT
MILCOM2005 Proceedings

[4] R. Overduin:
Trial of Mobile Communication in Urban Operations (in Dutch)
(Beproeving Mobiele Communicatie in Optreden Verstedelijkt Gebied)
December 2006, TNO report 34205

[5] *Tokyo Metropolitan Government Environmental White Paper 2006*
Chapter 2: Comparison of Cities in the World
www2.kankyo.metro.tokyo.jp/kouhou/env/eng/chapter2.html

[6] *The Spatial Distribution of Population in 35 World Cities*
www.bus.wisc.edu/realestate/pdf/pdf/
Bertaud%20and%20Malpezzi%20Part%20One.pdf

[7] ACTS CRABS study (pr.nr. AC215) D3P1B
Propagation Planning Procedures for LMDS (1999)

[8] 100 Largest Agglomerations in the World
en.wikipedia.org/wiki/List_of_metropolitan_areas_by_population

[9] S.B. Scherzer, S.D. Gordon, G.A. Martek, D. Ramakrishna:
A method for providing cellular system communication capacity increase
www.patentstorm.us/patents/7031754-claims.html

[10] D-Y Kim:
Antenna beam controlling system for cellular communication
United States Patent 20060192717
31 August 2006
www.freepatentsonline.com/20060192717.html

[11] *Smart Antenna Experiments for 3G and 4G Cellular Systems*
www.pentek.com/deliver/TechDoc.cfm/
3G4GCellAppl.pdf?Filename=3G4GCellAppl.pdf

[12] Hata and CCIR Formulas
w3.antd.nist.gov/wctg/manet/calcmodels_r1.pdf

[13] Y. Okumura, et. al.:
Field Strength and its Variability in VHF and UHF Land-Mobile Radio Service
Review of the Electrical Communication Laboratory,
Vol 16, Numbers 9-10, Sep.-Oct, 1968

[14] *Terrain Analysis Package (TAP) Propagation Comparison*
www.softwright.com/faq/engineering/Propagation%20Models.html

[15] V.S. Abhayawardhana, I.J. Wassell, D. Crosby, M.P. Sellars, M.G. Brown:
Comparison of Empirical Propagation Path Loss Models for Fixed Wireless Access Systems
VTC 2005

[16] Dariusz Wójcik:
Evaluation of near field of the GSM base station antennas in urban environment
Journal of Telecommunications & Information Technology 1/2003

[17] www.telsasrl.it/solutions/Cellular/Antennas/solutions_CellularANT.html

[18] www.skymasts.com/.../
skymasts-tetra-tetrapol-cdma450-antennas-accessories-product-catalogue.pdf

[19] Dr. G. Kamoto:
Radio Communications in Hostile Environments
SDRC, San Diego
www.virtualacquisitionshowcase.com/docs/SanDieg-Brief.pdf

[20] G.J. Timmermans:
Operational Context and Technical Architecture for the Mobile Domain
RNLA/Materiel Logistics Command
28 September 2006, Doc. ref. C3IA-TA-MD-VA

[21] C. Cerasoli (MITRE Corporation):
The Use of Ray Tracing Models to Predict UAV Air Relay Coverage in an Urban Area
MILCOM 2007, Florida October 2007

[22] O.J. Schuring, J.A.P. Smallegange:
Platform for Airborne Radio Relay Over Tactical Terrain (PARROTT), feasibility study- final report
Version 1.1, 11 November 2005

Annex B – MANET REPORT

The purpose of mobile ad hoc networks (MANET) is to allow for wireless multi hop communication. They are intended for situations where no pre-established communication infrastructure is available and the topology of the communication links may change dynamically, but can also be used to enhance or replace infrastructure based networks. Each node of the network should be used as a router to forward data to destination nodes that are not within radio communication range. Thus one of the central aspects in a MANET is the routing mechanism.

Depending on the field of application for the MANET there are several challenges to be considered. In [1] they are discussed for military application:

- Dynamic and rapidly changing topology
- Low available bandwidth
- Lack of a centralised entity
- Large network diameters
- Existence of unidirectional links
- Scaling up problems
- Security considerations for these shared medium access networks

[1] summarises: “These issues require that a routing protocol for a mobile ad-hoc network should be self starting and self organising, which provides the multi-hop, loop free paths to the required destinations in the network. Because of the mobility of the nodes, there should be a mechanism of dynamic topology maintenance, and rapid convergence of the protocol should be assured to stabilise the system. But the daunting task is to make it all possible using the minimum memory and bandwidth resources, and minimal overhead for data transmission. It is also required from these protocols to be scalable to large networks.”

As the above statement implies it is hardly achievable to design a MANET protocol which fulfils all requirements and meets all challenges. It is therefore of crucial importance to identify the set of (urban) scenarios a MANET protocol should be used for and create a specialised MANET protocol tailored to these scenarios. Such a specialised protocol adapting to different urban environments and conditions does not need to meet all the requirements as a generic protocol would have to and may therefore be easier to design.

In the following subsections we first describe the current status of mobile ad hoc network and then try to identify relevant issues that have to be addressed in future research. While the importance of these issues may vary depending on the scenarios the MANET protocol is used for, theses issues should be regarded whenever a MANET protocol is created.

Current Status of Mobile Ad-hoc Networks

While in earlier times the MANET subject was mainly discussed in the academic area, it also got more important in commercial products and solutions during the last few years. One reason for this development is that the MANET protocols are not seen in contrast to infrastructure based networks but as a complement, e.g. they can be used to connect several WLAN access points in a so-called Wireless Distributions System (WDS). Since there are many applications for a MANET, there are many different products and also different technological approaches. While some products implement the protocols on OSI layer 2 other products use implementations on OSI layer 3. Some products make use of standard protocols while others implement their own proprietary protocols. In some products the end user is part of the MANET and in other products, e.g. in a WDS scenario, the end user is only connected to a MANET node and therefore uses the MANET as a transfer network. Additionally some products make use of multi radio or multi channel approaches while others are restricted to a single channel. Many other criteria may be applicable to distinguish between the different products.

Currently, in the U.S. exist over 300 public projects where ad hoc networks are used or where it is planned to use them. The application of these networks has a range from public safety to public access. In the context of the Internet portal “global.freifunk.net” there are more than 250 registered communities which provide wireless mesh networks for internet access. The networks of these communities are mainly based on the work of three projects [2], [3] and [4] using the MANET protocols OLSR [5], HSLS [6] and SrcRR [7]. Another popular project is the “One Laptop per Child” project [8]. Its goal is to provide children around the world with laptops for educational purposes. These laptops shall have support for wireless mesh networks according to the upcoming IEEE 802.11s mesh extension [9] for the wireless LAN standard. It can be assumed that the usage of ad hoc networks will further increase in the near future, so that military ad hoc network may benefit from the progress in non-military projects. Especially projects in the area of public safety may be of interest.

Regarding the standardization of mobile ad hoc networks some approaches from IEEE and IETF exist. In the context of wireless LAN the upcoming extension 802.11s will introduce wireless mesh networking to the standard. The current draft specifies that conform radios must support the Hybrid Wireless Mesh Protocol (HWMP). This protocol is derived from the well-known AODV protocol and implemented on OSI layer 2. An important extension is that the protocol was extended with a proactive component. This extension is used for the discovery of a root station. This station can be used to provide the mesh network with access to the Internet or other networks. As an alternative the usage of other protocols, like the proposed Radio Aware OLSR (RA-OLSR), may be supported. Beside the definition of the routing protocol several other aspects, like congestion management, network access, multi channel support and security issues, are taken into account.

The IETF MANET Working Group [10] currently develops standards (RFCs) for reactive and proactive MANET routing protocols. The current approach for the reactive protocol is called Dynamic MANET On-Demand Routing (DYMO). The protocol is based on the earlier

approach AODV which was published as experimental RFC. Regarding the proactive protocol the previously published Optimized Link State Routing (OLSR) protocol is currently under revision and its second version (OLSRv2) is available as draft. The additional drafts PacketBB, SMF and NHDP include common aspects of the routing protocols, like packet format, multicast forwarding mechanisms and neighbourhood discovery, and publish them as separate standards the protocol standards will be referring to.

In the context of wireless metropolitan area networks the IEEE Working Group 802.16 (WiMAX) provides the standard extension 802.16e which allows for mobile recipients. If the network nodes are used in the mesh mode they can form an ad hoc network. Due to the usage of TDMA a time synchronisation of the nodes is necessary, but this also renders Quality of Service classes possible. Using TDMA requires that the medium access is controlled. There are two different scheduling mechanisms for the mesh mode: A centralised and a decentralised approach. In the decentralised approach the right to send data is agreed in the two hop neighbourhood of a node. The upcoming standard extension 802.16j will add multi-hop mesh networking capabilities and aims at increasing the overall coverage by adding meshed base stations. In the discussed scenarios the base stations are assumed to be stationary, so it questionable whether the meshed nodes of the final version of 802.16j can be mobile or not. All in all the two extensions make WiMAX more flexible and strongly increases the value for urban operations due to the added multi-hop capabilities. But it has to be taken into account that the relay stations are assumed to be stationary and that a solution with mobile relay stations may be preferable.

Important Issues for future MANETs for military use

Current approaches for mobile ad hoc networks often include only some aspects which are important for military use. While the aspect of a dynamically changing network topology is taken into account by most of the routing protocols, few protocols take the dynamics of link quality into account. Additionally aspects like transmit power control, data encryption and many others are only addressed by some approaches and there is currently no MANET approach which takes all important issues into account. In the following subsections we discuss aspects which should be solved in future MANETs for military use.

Security Aspects

In the context of security there are many new aspects to be considered for a MANET. Regarding the aspect of Denial of Service (DoS) the attacks from wired and also wireless networks are usually applicable in a MANET, while new attacks [11], [12] have to be considered. One of these new attacks can be directed against the topology information of the network. Even if a network is using encrypted management traffic, this traffic can be logged and replayed from another location. In an unprotected network this may result in a corrupted topology information introducing possibilities for black hole and other attacks.

Beside of DoS attacks, tracing the management information and the transferred data of the network may uncover the topology and possibly identify important network nodes for unauthorized stations. While the encryption of the management information and the traffic

data is fundamental to hide the content of the information, it may be of interest to hide the type and the amount of data transmitted. Due to the shared medium of a MANET enemy nodes can easily listen to the traffic. Such a node may then draw conclusions from the size, the timing and the frequency of network traffic, which may help to differentiate between management and data traffic, to identify important data streams and maybe their origin and/or their destination [13], [14].

As already stated before the encryption of management information and transferred data is essential. To guarantee secure encryption an adequate mechanism for exchanging and updating an encryption key is needed. This mechanism has to be able to cope with separated network parts. These parts may be separated for a short period of time, so that a common key may still be valid, and also for a longer time, so that the old encryption has become invalid. If the key has become invalid, aspects like merging the separated network parts have to be solved.

In addition to intrusion prevention mechanisms a network should also be able to deal with intruders which were able to circumvent the barriers by encryption and other proactive security mechanisms. While there are many solutions for intrusion detection in wired networks, the aspect of intrusion detection in a MANET [15] has to be further investigated.

Quality of Service and Congestion Control

A critical aspect regarding current MANET protocols is that they may perform well under low and medium network load, but cannot adequately cope with high load and an overloaded network. There are multiple possibilities to address this problem. One way may be to avoid congested regions in the network by using an adapted routing metric. Improved routing metrics may also be used to improve the behaviour under low and medium load. Another way can be to control the network access. This may be realized by using prioritization to distinguish between important and less important data and the less important data can be dropped under high load. But due to the dynamic network topology and the dynamic behaviour of network links it is hard to proactively decide whether there is high load on the network or not. Closely coupled to this problem is how Quality of Service (QoS) guarantees can be made. While for some network types, like TDMA based networks, delay guarantees can be made for single hop wireless connections, it is hard to predict the delay and keep guarantees if the number of intermediate nodes is not known a-priori and may change over time. Additionally aspects like a changing network load influences endpoint connections. All in all there are currently many unsolved issues regarding QoS in MANETs.

Scalability / High Data Rates over multiple hops

Due to the shared medium approach used in current MANETs the data rates provided to a single node is reduced from transmissions of adjacent nodes. Therefore the maximum supported rate depends on the activity and the density of nodes in the vicinity of a transmitting node. Since the action of relaying information is also an activity to the surrounding nodes, a higher number of hops further reduces the maximum available data rate. As indicated by this observation, MANETs scale poorly with the number of nodes, concurrent

traffic and the number of hops used [16]. Since these problems are inherent to MANETs it is an important task to improve the overall capacity of a MANET to counter the scalability effects and render higher data rates possible.

This task may be accomplished in several ways. One way could be to improve the radio and therefore increase the data rate for each link. Additionally as already introduced in some protocols like [17] the usage of multiple channels or multiple radios can be used to increase the capacity. Another approach can be to control the load on the network. This can e.g. be done by controlling the transmit power thereby reducing the interference radius of nodes [18] or by using multi rate capable radios which use higher data rate modulations if the distance between two communicating nodes is small [19]. Another solution might be to use routing mechanisms to automatically select routes which lead to a low load on the network [17], [20]. To achieve this, a routing mechanism has to estimate some kind of quality value for different routing paths. The determination of such a quality value must be well-investigated since there are multiple side-effects on other critical aspects like the reliability of a link.

Multicast Support

A frequently mentioned requirement for MANETs in military scenarios is the capability to support multicast traffic. While there are first approaches to fulfil this requirement, future approaches have to address the other aspects described before. As an example for a current approach the Simple Multicast Forwarding (SMF) protocol [21] introduced by the IETF performs multicast transmission by flooding the network. It supports different flooding mechanisms, which reduce the load on the network compared to classic flooding, but multicast transmissions still create load on the whole network. Thus it is questionable whether this protocol can be efficiently used in larger MANETs. Additionally their reliability may be a critical issue. While the flooding process often introduces redundant packets and therefore introduces some kind of reliable transmission, there are scenarios, like a chain of nodes only reaching their direct neighbours, where no additional redundancy is introduced which may lead to a lower reliability. Regarding multicast communication it is important to develop protocols that explicitly address all other important issues.

Conclusion

In their current state MANET solutions are only of limited use for military purposes. While there are some civil commercial products available, these products cannot fulfil all requirements of military communication systems. Current approaches for standardization, as observed in the IEEE and IETF, may be beneficial for the future development of these products, but it cannot be expected that all important issues will be solved in this context. It is therefore of special importance for future research that the exact requirements for different military scenarios are determined and specialised protocols for these scenarios are developed. Although not all of the above issues must be solved for every scenario these issues can be used as a guideline for the research which has still to be done and should intensified.

[1] IST-035/RTG-015, Final Report “Awareness of Emerging Wireless Technologies: Ad-hoc and Personal Area Networks, Standards and Emerging Technologies”,April 2007

[2] Freifunk Community Berlin - http://berlin.freifunk.net/

[3] Champaign-Urbana Community Wireless Network - http://www.cuwireless.net/

[4] MIT Roofnet Project - http://pdos.csail.mit.edu/roofnet/

[5] T. Clausen and P. Jacquet, “Optimized link state routing protocol (OLSR)”, RFC 3626, IETF, 2003

[6] C. A. Santivanez, R. Ramanathan, “Hazy Sighted Link State (HSLS) Routing: A Scalable Link State Algorithm”, BBN Technical Memorandum No. 1301, BBN Technologies, August 2001

[7] J. Bicket, D. Aguayo, S. Biswas, R. Morris, “Architecture and Evaluation of an Unplanned 802.11b Mesh Network”, In ACM MobiCom, 2005

[8] “One Laptop per Child” Project - http://laptop.org/index.de.html

[9] IEEE 802.11 Working Group – http://www.ieee802.org/11/

[10] IETF MANET Working Group – http://www.ietf.org/html.charters/manet-charter.html

[11] S. Avancha, J. Undercoffer, A. Joshi and J. Pinkston. “Security For Wireless Sensor Networks”. Chapter 12 in “Wireless Sensor Networks”, pages 253-275, Springer US, ISBN 978-1-4020-7883-5

[12] M. Jahnke, J. Toelle, A. Finkenbrink, A.Wenzel. „Methodologies and Frameworks for Testing IDS in Adhoc Networks“. To be published in The 3-rd ACM International Workshop on QoS and Security for Wireless and Mobile Networks, Greece, October 2007

[13] J. Kong, X. Hong, M. Gerla. „A new set of passive routing attacks in mobile ad hoc networks“. IN: MILCOM 03, October 2003

[14] J. Kong, X. Hong. “ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks”. In Proceedings of ACM MobiHoc 03, June 2003.

[15] A. Patwardhan, J. Parker, A. Joshi, A. Karygiannis and M. Iorga. Secure Routing and Intrusion Detection in Ad Hoc Networks. In: Third IEEE International Conference on Pervasive Computing and Communications, Kauaii Island, Hawaii, March 8-12, 2005.

[16] J. Sucec. “Routing in mobile ad hoc networks: Scalability, Resource Management and Application”. PhD Thesis, New Brunswick, New Jersey, May 2003.

[17] R. Draves, J. Padhye, and B. Zill. “Routing in Multi-radio, Multi-hop Wireless Mesh Networks”. In ACM MobiCom, Philadelphia, PA, September 2004.

[18] M. Gerharz, C. de Waal, M. Frank, P.Martini. “Influence Of Transmission Power Control On The Transport Capacity of Wireless Multihop Networks”. Proc. of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 1016-1021, Barcelona, Spain, September 2004.

[19] T. Bachran, H. H.-J. Bongartz, and A. Tiderko, ”A framework for multicast and quality based forwarding in MANETs”, in CCN: Proceedings of the 3rd IASTED International Conference on Communications and Computer Networks, ACTA Press, 2005.

[20] Douglas S. J. De Couto. „High-Throughput Routing for Multi-Hop Wireless Networks“. PhD Thesis, MIT, June 2004

[21] SMF Design Team and IETF MANET Working Group, “Simplified Multicast Forwarding for MANET“, Internet draft, IETF Network Working Group, draft-ietf-manet-smf-07.txt, August 2008

Annex C – BOWMAN LIMITATIONS FOR URBAN OPERATIONS AND POTENTIAL SOLUTIONS

IMD Department

William Gorst
Information Management
Bldg 5, Room 202, i-Sat E,
Desk 142
DSTL Porton Down
Salisbury, Wilts, SP4 0JQ

T: 0198065 8847
F: 0198065 8600

wdgorst@dstl.gov.uk
www.dstl.gov.uk

Dstl is part of the
Ministry of Defence

Date:29 March 2010

Document Title

Bowman Limitations for Urban Operations and Potential Solutions

Report Classification Level: UK RESTRICTED

Unclassified Report Summary

Users of Bowman Very High Frequency (VHF) Combat Net Radio are frequently unable to communicate with one another in urban environments due to poor radio frequency coverage. In order to maintain communications between personnel and HQ, manual (verbal) relay is required. This results in an increased need for equipment and puts personnel at significantly greater risk.

To quantify the extent of this problem, a path loss prediction algorithm has been used to examine propagation in urban areas. The results are consistent with user observations that VHF communications in urban areas are highly variable. Propagation along streets could allow a communications range of several kilometres between users, whereas penetration into built up areas might limit the range to 200 metres or less.

Communications coverage could be increased by deploying relay stations, ideally located above ground level, for example on top of a tall building. However, the station may need to be manned in order to minimise the risk of theft or destruction. Airborne deployment is considered. Other potential solutions include the use of a propagation tool to quantify the extent of the problem prior to deployment, deployment of an expendable unattended relay, exploitation of any existing mobile phone infrastructure and the employment of Bowman High Capacity Data Radio (HCDR) to provide Voice over Internet Protocol (VoIP). It is noted that any solution should ideally be organic to the users and provide both a reliable and persistent capability.

For access to this report contact DSTL at the contact information provided above.

Annex D – NETWORK EVOLUTION UNDER NNEC CONCEPTS

SELEX Communications
A Finmeccanica Company

NETWORK EVOLUTION UNDER NNEC CONCEPTS
TECHNICAL STUDY

Date: 30/07/2007

Higher thinking.
FINMECCANICA

Table of Issues		
Rev	Date	Description
00	30/07/2007	DRAFT

SELEX Communications
A Finmeccanica Company

TABLE OF CONTENTS

Table of Figures

1. INTRODUCTION

1.1 References

[1] NATO Network Enabled Capability Feasibility Study – Vol. II Version 2.0
[2] Draft NNEC Force Proposal 2008

1.2 Objective of the Work package

This work package addresses the developing of the Networking and Information Infrastructure (NII) in a telecommunication network environment, lying on the framework used by NATO and NATO Partner Nations, and described in the NATO NEC Feasibility Study (NNEC-FS), to guide the planning and development activities.

The final aim is to start suggesting some preliminary areas of intervention on the communication assets currently in use to launch a migration process such to be in line with the technological trends already clearly identified by NATO as key player in the NNEC transformation.

1.3 Document contents

The document is basically organised in three main sections:

- the first part (Chapters 2 and 3) defines the scenario and summarises the NATO point of view as acknowledged by Selex Communications
- the second part (Chapters 4 and 5) defines the guidelines for the development of the NII and suggests short term achievable scenarios with a focus on the technological areas
- the third part (Chapter 6) identifies possible areas of intervention for beginning a transformation process as much as possible stuck to the network-centric framework and, in the same time, clearly to recognise short-term implementation achievements

The document is mainly focused on the Communication Services and System Management of NII and only makes reminds to aspects related to the IIS services which are expected to be treated separately and, mainly, within the framework of a possible NCW Study.

Two specific issues are treated in separated appendixes to this document: the evolution of NII deployable and mobile segments and a hypothesis of migration and roadmap in phase towards Everything over IP from smooth integration on of VoIP, VoSIP, Secure VoIP and IPv4, dual stack IPv4/IPv6 towards IPv6.

1.4 Abbreviations

FAS	Functional Application Service
FS	Feasibility Study
NATO	North Atlantic Treaty Organization
NEC	Network Enabling Capability
NII	Networking and Information Infrastructure
PDH	Plesiochronous Digital Hierarchy
SCIP	Secure Communication Internet Protocol
SLA	Service Level Agreement
SDR	Software Defined Radio
NNEC	NATO Network Enabled Capability
NNEC-FS	NNEC Feasibility Study
NCW	Network Centric Warfare
VoIP	Voice over IP
SVoIP	Secure VoIP
VoSIP	Voice over Secure IP
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
TOA	Transformational Objective Areas
CIMIC	Civil-Military Co-operation

2. SCENARIO

2.1 Operational needs

The NATO NC3 Board has recognized the need of developing and adapting the NCW concepts and the NEC capabilities to the NATO context.

In this scenario, it is therefore recognized by NATO nations the need of activating a study process which in some way adhere to the NATO NC3 Board guidelines and evaluate the applicability of the NNEC concepts to the transformation of the military assets in national context.

The main target is to increase the effectiveness of NATO structure in facing the new missions and in reacting sinergically to the new security challenges.

The enhancement of new NCW/NEC capabilities (Situation Awareness, etc) by a NRF in conducing missions leads to a number of new requirements, mostly referable to C4ISR systems, which are analyzed and defined as recommendations by the NNEC Feasibility Study developed by NATO.

NEC capabilities, mandatory for the achievement of the above mentioned target and identified as “Transformational Objective Areas” (TOA) in the NNEC-FS are:

- Effective Engagement
- Information Superiority
- Expeditionary Operations
- Joint Manoeuvre
- Enhanced CIMIC
- Integrated Logistics

and include the connection on a Global Network of Sensors, Decision Makers and Effectors in a multinational context, military, governmental or not, dedicated to collaboration activities such as planning, validation and execution.

Therefore, the NEC capabilities must be able to grant key-players to carry out effective and secure information exchanges, using communication networks interconnected, interoperable and robust which are able to support effectively the collection, the analysis, fusion and sharing of the information.

2.2 Transformation process strategy

The strategy to meet such operational needs and therefore to realize the transformation process towards NCW/NEC capabilities can be based on the following approach:

- Development of a national NCW/NEC capability and introduction of the related new concepts by taking into consideration the guidelines and the Roadmap approved in NATO, properly modified to meet the needs and ambitions of a Nation, also by envisaging their extension to the Home Land Security and Urban Operations.
- Creation of a dedicated Organism in the Defense able to grant, by means of M&S tools and industrial partnerships, an unambiguous direction for the definition and the realization of the National C4ISTAR architecture which has to be taken as the mandatory step to enhance the capabilities of the Defense and to support the transformation towards NCW/NEC and the execution of international missions.
- Improvement of the Centers of Excellence of the Defense and of the Industries as well in order to maximize the support for the development of systems and their validation/certification; harmonization and integration of their IT platforms and the connection with similar international entities is also important

2.3 This study

Target of this study is to present an overview which identifies possible areas of intervention in order to support the evolution in the short term of the current Defense network(s) towards the “Infostructure”, that is towards a network model which, thanks to its networking capabilities and provided services (“core services”) is the basic element to support network-centric operations.

The final target of the approach to NCW/NEC is to achieve an increase of interoperability among networks which take into account the NATO NEC Feasibility Study recommendations and the national operational needs.

In particular, the interoperability to be achieved has to be conceived as the capability of networks of operating jointly in an effective way according to the Networking and Information Infrastructure (NII) principles defined by NATO within a new architecture framework.

The overall process represents for NATO countries a very big challenge which has to be faced in a structured way and it requires a significant effort in term of planning, validation and implementation by the Defense Organisms and the industrial partners.

For this reason, the aim of this study is to put the focus on the concepts underlying guidelines to apply at national level, transformation methodology and short-terms areas of intervention, envisaged on the basis of the experience matured by Selex by operating in the international and home-country scenarios.

This should provide useful indications to the Customer about the NATO doctrine and technological trends and the approach as recognized by Selex Communications to the NNEC transformation of communication systems/platforms.

2.4 NCW/NEC Study with Defence and Industry Partnerships

As primary goal, a High Level Communication Architecture has to be defined to achieve a global view of the current scenario of the communication systems. It is therefore to start with an information collection campaign in order to build up a package of data related to the communication assets currently in use and their functional and connectivity characteristics.

This task, even though very time and resources consuming, has to be considered a mandatory task because it represents the starting point for the next phases of the study aiming at identifying the areas to be approached and the pragmatic proposals of update in the network-centric framework.

Then, taking into account the documentation on the NCW transformation and after having analyzed the specific national needs, the national network-centric transformation can be defined.

The national guidelines describe the evolutionary transformation path towards the long term target represented by the network centric “Infostructure”.

From these guidelines, it is then achieved the “short-term scenario”, that is a view of networks and systems have to look like in order to meet the first phase of the networ-centric transformation process.

The definition of actions comes from the comparison of the short-term scenario and the maturity level of the current assets compared to this scenario (current baseline).

The evaluation of the maturity levels of networks/systems compared to the short term target requires applying an evaluation methodology of interoperability among communication assets suitable to focus on those parameters of specific NCW interest.

To this aim, the main interoperability analysis models available in literature can be used. The emerging criticalities allow pinpointing the areas for short-term intervention.

In brief, a study activity should aim at defining a detailed migration Plan of current resources throughout an analysis of current resources (for tactical and strategic networks and C2 Systems, Sensors, Platforms) and their level of interoperability and then at defining a reference plan (a roadmap) for the evolutionary development of national NCW/NEC capabilities that can be foreseen in the future scenario.

After that, the description of the current configuration of the national C4ISTAR architecture followed by the step-by-step definition of a preliminary reference NCW architecture. For this activity, methodologies recommended by international Organisms, such as NATO and the US DOD, has to be adopted (respectively NAF and DODAF), supported by Modeling & Simulation tools as applicable.

This reference plan includes also the analysis of possible synergies between Defense and Industries, fundamental to manage as effectively as all NATO countries, The NCO transformation process.

3. NATO-NII GUIDELINES – NNEC FEASIBILITY STUDY

The Networking and Information Infrastructure (NII) is the information infrastructure which will allows the Armed Forces to operate in accordance with the Network Centric Warfare principles.

Target of the NII is to carry out one single communication network for the fixed and tactical components, able to deliver information to users who need it, by taking into account the actual needs in terms of priority, time delays and security.

The infostructure is independent by the platform application software (Functional Application Services) and, in addition to the provision of IT services to the users, it supports the information exchange necessary to the Command and Control applications.

The NII is based on a Service Oriented Architecture (SOA). The structure is modular and each component carries out a service, provided to the requiring entity which can be another service or an application.

The NII services involve four technological areas: telecommunications, information, information assurance and system management. The following figure allows identifying the NII in the wide scenario of the areas involved in the NCW transformation of the NATO Armed Forces.

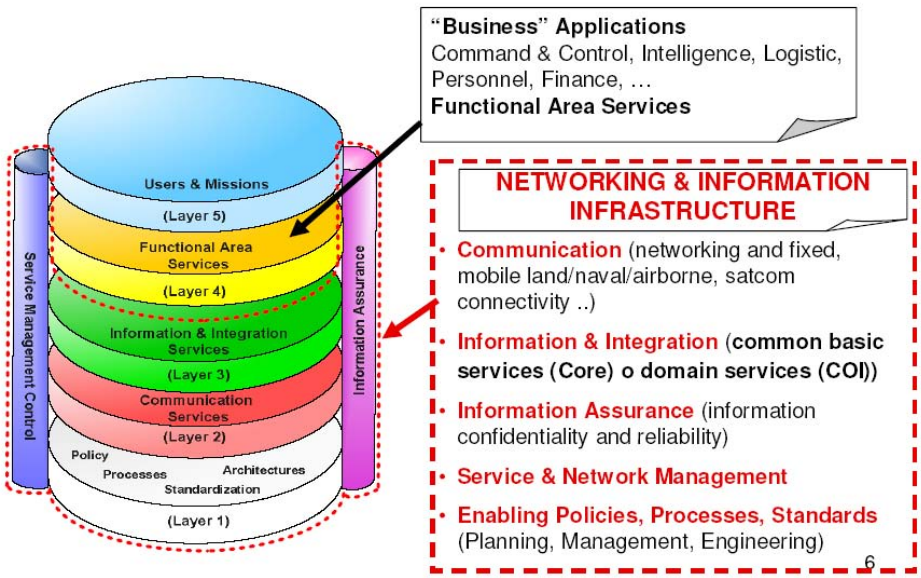


Figure 1 – NII (infostructure)

Communications, intended as transport services of the exchanged traffic, represent the *backbone* of the NII.

From the networking point of view, with an approach similar to that adopted in the World Wide Web, networks based on heterogeneous technologies and protocols can achieve interoperability by using a common language, the IP protocol, and thus by creating a seamless network extended from the infrastructure segment to the mobile segment down to the dismounted soldier on battlefield.

The Information & Integration Services layer is composed by three sub-layers: the COI services, the core services and the IIS infrastructure services.

IIS are software components designed to be used on heterogeneous platforms and accessible on the network by means standard protocols; they are divided in services for specific users' groups, namely "COI (Community Of Interest) Services", and common utility services named "core services".

The IIS infrastructure services provides the higher layers with all those mechanisms necessary to carry out distributed processing and data sharing in the network. Services like web browsing (HTTP) and file transfer (FTP) belong to this category.

Information Assurance includes all the tools finalized to the protection of the information on the network.

System Management and Control has the main task of delivering "End to End" services while the technical management and control, extended to all the elements of the Infostructure, are under the responsibility of the system managers (for each system), which keep their operational independence.

All the components (layers) part of the NII is characterized on the basis and depending on the specific segment (infrastructure, deployable and mobile) which the component is applied to. Such characterization must anyway to grant the availability of the end-to-end services.

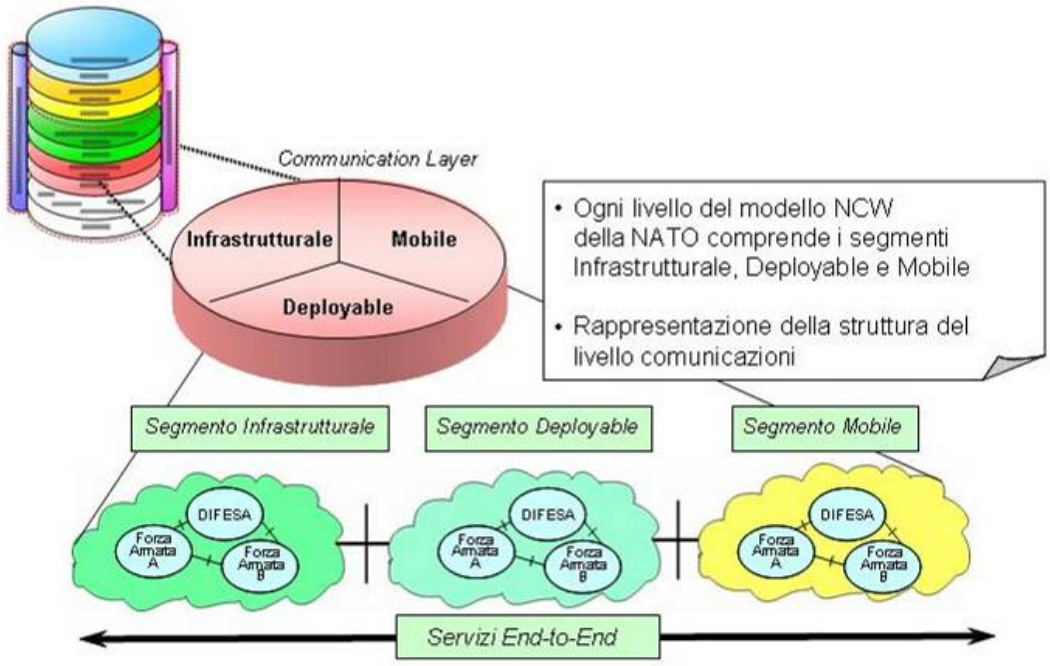


Figura 3.2 - 2. NATO NII – details of the communication layer

By taking as reference the contents of the NNEC-Feasibility Study, it is possible to identify the guidelines for the network-centric migration process for each one of the four NII components.

3.1 Communication services

Reference is specifically made to [1], Vol.2, Chapter 3.

The Communication Services Layer is subdivided into Transmission Services and IP Services.

Transmission services encompass such areas as satellite communications, wireless services, tactical data links, and fixed wired infrastructure.

The study identifies the following main guidelines per communication area:

- **Wideband wireless**: usage of standard and portable waveforms. Software Defined Radios (SDR) is seen as a key enabler for coalition waveform interoperability, that is referred as the technology able to grant the future interoperability on the battlefield.
- **Ad-hoc networking:** developments of network protocols allowing the integration in the NNEC IP network of high mobility users or other application specific networks (example, sensors' networks).
- **SATCOM**:
- **Capacity including Bandwidth**: In order to operate in a fully networked way, the NNEC clients, whether these are machines or humans, will need communications capacity, normally specified in terms of bandwidth, more than they have today. Therefore networks should use SLA schemes and associated capacity management.
- **Black Core Network**: realization of a secure backbone network able to support multilevel encrypted traffic and IPv4/IPv6 dual stack, possibly achieved by federating more than one "black core networks".
- **Quality of Service:** the convergence of services over IP implies the need of managing QoS in accordance with Service Level Agreements (SLA) contracted with the users.
- **IP Encryption**
- **Everything over IP (EoIP):** convergence of traffic related to voice, data and video services over IP which will have to be the common transport mechanism, able to meet the QoS requirements of the applications;
- **IPv6:** IPv6 is considered the reference protocol for the NII network in the long term, which is the protocol that will make possible the convergence of all the services, including those requiring very constraining QoS, over one single typology of network. The introduction of this protocol is foresee by throughout a gradual process that, in the short/medium term, will let IPv4 and IPv4/IPv6 dual stack systems to coexist in the network.
- **"Plug & Operate" capability**: that is the support to mobility of the operational units that, moving in the network, always have access to services they need, with no need of manual reconfigurations.
- **Edge Proxies:** main enabling factor of the integration of non-IP networks in the IP network. Placed on the edge of the IP network, they perform the task of interfacing civilian and military networks based on technologies different than IP.

3.2 Information & integration services

Reference is specifically made to [1], Vol.2, Chapter 4.

- **"Need to share" instead of "need to know"**: the focus is moved from the Information Exchange Requirement (IER) of each network node to the availability in the network of the information needed by the nodes.
- **Service Oriented Architecture** (SOA)
- **Core services**: defined as those basic information services (Enterprise Service Management, Messaging, Discovery, Mediation, Collaboration, Storage, Information Assurance, Application, User Assistance) that can be used by any user, service or application on the network. These services are "building blocks" for the development of specific services (COI services) or applications (FAS) and, with communications, realize the infostructure.
- **Metadata** (XML and "XML-enabled" technologies): main enabling factor of the information exchange on the network by means of Web Services.
- Secure sharing of "text-based" information
- Common Data Model: standardization of the metadata
- use of "open standards"
- Information Exchange Gateway (IEG): in order to achieve the interoperability with legacy services and towards NATO.

3.3 Information assurance

Reference is specifically made to [1], Vol.2, Chapter 5.

- Security on the "edge": i.e. moving the network security services towards the final user (as an example encryption, authentication)
- Key Management Infrastructure (KMI)
- Multilevel security
- Cross-domain Core Services
- Dynamic, role-based and policy-based access to information (medium term): development of PKI mechanisms and XML technologies.
- Information labeling
- Strong Authentication (for terminals and users)
- Secure QoS: granted end to end QoS for information flows crossing networks with different levels of classification.

3.4 System Management and Control

Reference is specifically made to [1], Vol.2, Chapter 6.

- Management and control in an integrated and secure way of the end-to-end services
- Service Level Management: management of “contracts” between user and network for the user of services with given parameters of Quality of Service. The compliance with the SLAs agreed with users is the target of the Management and Control service, as well as the reference element for the system performance analysis.

4. GUIDELINES FOR THE DEVELOPMENT OF THE NII

As already said above, the network centric migration process must be approached in a incremental way, according to a timeframe to be agreed.

In the following, this section tries to trace the technical and functional guidelines for the development of a network-centric infostructure for each component introduced above:

- Communication services;
- Information & Integration Services
- Information Assurance
- System Management and Control

The Communication services area is then split in the segments Infrastructure, Satellite, Deployable and Mobile. This subdivision will be kept as possible in the whole document.

Since the technology trends in the future 10-15 years cannot be foreseen in their details, it has to be assumed as common guideline for all the technological areas that maximum effort be spent in keeping the architecture as open as possible in order to allow the introduction of new technologies once they become applicable.

4.1 Communication services

4.1.1 Infrastructure Segment

The transformation process of the communication concerns the whole segment of the infrastructure networks, both access and transport/backbone network.

Each communication service (either data, voice or video), will be delivered over IP traffic streams and will be managed as end-to-end by suitable management systems able to optimize the use of the network resources on user request basis and able to operate automatic re-engineering in case of faults on the network.

The migration of various types of network traffic over a unique protocol, the Internet Protocol, implies the simplification of the network with clear advantages in terms of interoperability among networks with different transmission technology, of network resources usage, reduction of investments (economy of scale) and exercise (standard equipment).

The key technology of this network will be IPv6 which, due to its intrinsic features, seems to be the one who will carry out the convergence of all the services over one single networking protocol, by solving the problem of the support of the QoS.

The transport infrastructure will have to able to make the QoS management performed as easy as possible by granting to the information flows the required bandwidth.

Besides technologies and protocols, the network architecture will be of the most importance.

The infrastructure communications will be based on a wideband national backbone which in turn will be based on optical technologies, with backup over microwave radio relays, for the transport of traffic between access networks.

According to trends highlighted by NATO, this backbone will operate as a “black core network”. Inside the black core network, both classified and unclassified information will be delivered, with a number of classification levels. Classified information will be transported in IP streams encrypted by multi-level encryption devices to the edge of the network. Such devices will grant the security of the exchanged information and will have to operate without affecting at all the performances provided by the network in terms of QoS.

In the short term, a migration can be started based on the following tenets:

- The circuit switching will be replaced by the packet switching, which allows a dynamic management of the bandwidth.
- The switching in the network nodes must support the traffic QoS requirements. To this aim, mechanisms will have to be adopted for mapping and management of the QoS requests from application to IP packets and from IP to the lower layers.
- Taking into account the current very wide use of the IPv4, the trend is to plan the acquisition of IPv4/IPv6 dual stack equipment, able to startup the migration towards a full-IPv6 network while keeping the compatibility with IT and network devices already procured.
- The use on large-scale basis of fiber optics will be matched with the introduction of DWDM (Dense Wavelength Division Multiplexing) equipment in order to increase the transmission capacity of the optical links.
- The use of “wideband wireless” solutions, in order to increase the access capacity of nodes not connected to F.O.
- Moreover, in order to increase the network reliability also at physical level, automatic protection/”bypass” devices will have to be considered in order to grant the path availability in case of fault.

4.1.2 SATCOM Segment

The long term target is a broadband full IP SATCOM network with QoS management. It will be possible to support the capacity increase and optimization by the use of on demand satellite bandwidth and Ka and EHF bands. This network will have to be able to support on the move SATCOM by means of compact satellite terminals and On The Move (OTM) capabilities.

4.1.3 Deployable segment

The network centric migration of the deployable segment communications will follow trends applicable to the infrastructure segment, i.e. communications based on IP protocol as convergence layer and transported by a “black core” with the encryption devices positioned on the edge of the system.

Deployable networks as well must therefore in some way start this process towards the full-IP architecture with a smoooth and step-by-step migration of voice, data and video among Command Posts.

The support of the QoS, a critical issue due to the characteristics typical of land tactical wireless links, will reasonably keep on relying in the short term on lower layer connection-oriented protocols based.

In addition, the deployable networks, currently conceived to cover very wide areas with a high connectivity ("meshed" networks), will evolve to more slim structures, with less connectivity to support Post Commands distributed in operational areas.

The traffic generated by deployable nodes, moreover tipically growing in netcentric contest, wiil be conveyed on a few links regardless those available in a fully meshed network and will be therefore necessary to upgrade transmission capabilities through progressive introduction of Broadband Wireless links.

4.1.4 Mobile Segment

One of the most exciting challenges of NCW is to allow an operator on the battle space, either on vehicle or dismounted, to have access to the same set of services available in the infrastructure environment.

To achieve this target it is necessary to increase the transmission and processing capacity available to the mobile segment one side, the other side it is mandatory to manage the integration of the mobile platforms in the network-centric environment, by empowering them with IP networking capabilities.

Therefore the migration has to be developed in parallel on the vehicular platforms and "soldier platform".

In the short term, it is necessary to increase the transmission bandwidth available on vehicles.

Introducing a Broadband Radio is the solution identified in order to fill the so called gap capabilities. The use of this mean grants a communication bearer which is suitable to the information exchange among vehicles and among vehicles and shelters, in terms of bandwidth and usage of the IP protocol. This system enhancement, with the mobility support represents the first step to achieve a MANET (Mobile Ad-hoc NETworking) capability.

From the "soldier platform" point of view, the first step to achieve a network-enabled soldier has to be done by developing and deploying a NEC platform for the dismounted units (corresponding to the "Soldato Futuro" system in development for the Italian Armed Forces).

Tactical communications will be progressively empowered with the introduction of the "Software Defined Radio" (SDR). This technology will grant, together with unique characteristics of flexibility and interoperability, broadband, security and reliability to the battle space communications. This introduction will also be the key enabler for the extension of the IP technology to the mobile segment.

With the deployment of the first SDR systems, in the medium term a full MANET capability will be made available, with multi-hopping and auto-reconfiguration (self-reconfiguration, adaptive-configuration) network functions, key factor to transform also high mobility platforms into network enabled nodes.

MANETs will allow, applied to the vehicular node and to the soldier node, amplifying the operational capabilities of the means, by exploiting at the maximum extent the on board transmission equipment features in order to keep the crew always connected, whatever is their position and, at individual level, they will allow

the user to be always connected to the other Squad mates and to the Squad Commander to communicate seamlessly with the NEC network, in all the operational conditions and in a completely automatic way.

The *broadband wireless* will complete the coverage of the tactical environment which will be crossed by bulk traffic flows aiming at making concrete the “information superiority”.

In addition, the final stage of integration of the mobile networks with deployable and infrastructure assets, by extending the information QoS management capability in theater as well, this way allowing communications with granted quality from the strategic command to the soldier.

4.2 Information & integration services

The new concept of network given by the NATO guidelines envisages an infrastructure able to provide users, in addition communication capabilities, with a set of information services, both services specific to groups of users (COI) and basic services (“core services”).

“Core services” are grouped in the following categories:

- **Application**: Hardware/ Software environment for development, test, installation and maintenance of distributed applications,
- **Discovery**: discovery and access to network elements, data, users and services,
- **User Assistance**: assistance services to the users via the system (Help on line, wizards, management of preferences, etc),
- **Collaboration**: services for collaboration and sharing information such as audio/video conferencing, file exchange, sharing of texts and images,
- **Storage**: storage, management and archiving of data,
- **Mediation**: capabilities of processing, translation and delivery of information among the various entities in the system,
- **Messaging**: E-Mail and formatted messages,
- **Enterprise Service Management (ESM)**: management and monitoring of the system elements,
- **Information Assurance (IA)**: necessary to grant constant and reliable levels of security: authentication, encryption, key management, etc.

These services, with transport and networking layers, will realize the “common environment” on which each node of the NCW network will base its own communication and information management capabilities

The availability of such services will have in the long term be grant both on the classified and the unclassified networks, from the Strategic Command down to the operator on the field with the proper variations in terms of enabling technologies and down-sizing of the solutions.

Such services will be realized according to a SOA model in order to be independent from the hardware platforms, operating systems and programming languages: this will allow achieving a universal interoperability of services.

The migration towards the final target will be in phases depending on the current availability of bandwidth and the maturity of technologies.

In the short term, the first to start the process will be the infrastructure segment and the part of deployable segment where processing and connectivity capability will be sufficient to support the distribution of the Core Services.

When technologies enabling the SOAs in low rate, poor connectivity and limited processing capability environments will reach their maturity, core services will be extended to the mobile users as well.

Interoperability at “Core Services” leve with legacy networks and NATO/EU will be achieved by means of proper “Information Exchange Gateways” (IEG).

4.3 Information assurance

The network centric migration implies a progressive increase of the amount of information available to users and the need of realizing dynamic Communities Of Interest (COI). This will require redefining and enhancing the network, the exchanged data and user’s security services.

In order to meet these requirements, it will be necessary to implement the end-to-end protection of the communications, for instance by integrating the encryption in the user terminals, and to allow a higher flexibility in the management of the secure users, by realizing a Key Management Infrastructure (KMI) for the automatic management of the encryption keys and digital certificates.

In addition, the introduction of multilevel security solutions will allow managing information at different classification level, this way converging in one single IT infrastructure the networks with different classification, today physically separated.

All the security mechanisms will have to operate transparently to the user, this way by not affecting at all the network performances in terms of QoS.

The evolution of the current security services will require a clear planning in order to minimize the impact on operational networks and therefore saving the investments.

In the short term it is wise to start evaluating the use of dual stack IPv4/IPv6 IP crypto which grant interoperability with the IP crypto currently in use and are able to support data flows more and more bandwidth demanding and in compliance with the increase of bandwidth on the communication infrastructure.

Together with the introduction of this new generation of IP crypto, which allows protecting communication among classified LANs, it has to be considered the use of devices supporting the SCIP in order to allow other users connected to unsecure PSTN, ISDN and IP networks to setup a secure connection for voice and low rate data.

Both IP crypto and SCIP devices will require the introduction of mechanisms for the management of keys and digital certificates. In the short term, a key distribution system will have to be used and PKI infrastructure will have to be defined.

In the medium term, the large scale use of high rate dual stack IP crypto will have to be completed and user authentication mechanisms will have to be introduced as well as the integrity check and the protection of information. Initial “multilevel security” solutions will have to be introduced.

All this will be supported by a KMI, at national level, such that includes the PKI and the key distribution systems implemented in the short term.

In the long term period, very high capacity encryption devices (Gbps) will be needed, likely full IPv6 and where possible integrated in the user terminals. The multilevel security devices will have to be fully integrated in the infrastructure and the

access to networks and information will have to be managed by means of digital certificates; therefore the KMI infrastructure will have to reach full maturity.

4.4 System Management and Control

The System and Network Management will have to operate in a distributed and cooperational way, in order to allow every network manager keeping its own operational autonomy even though under the control of a central administration authority.

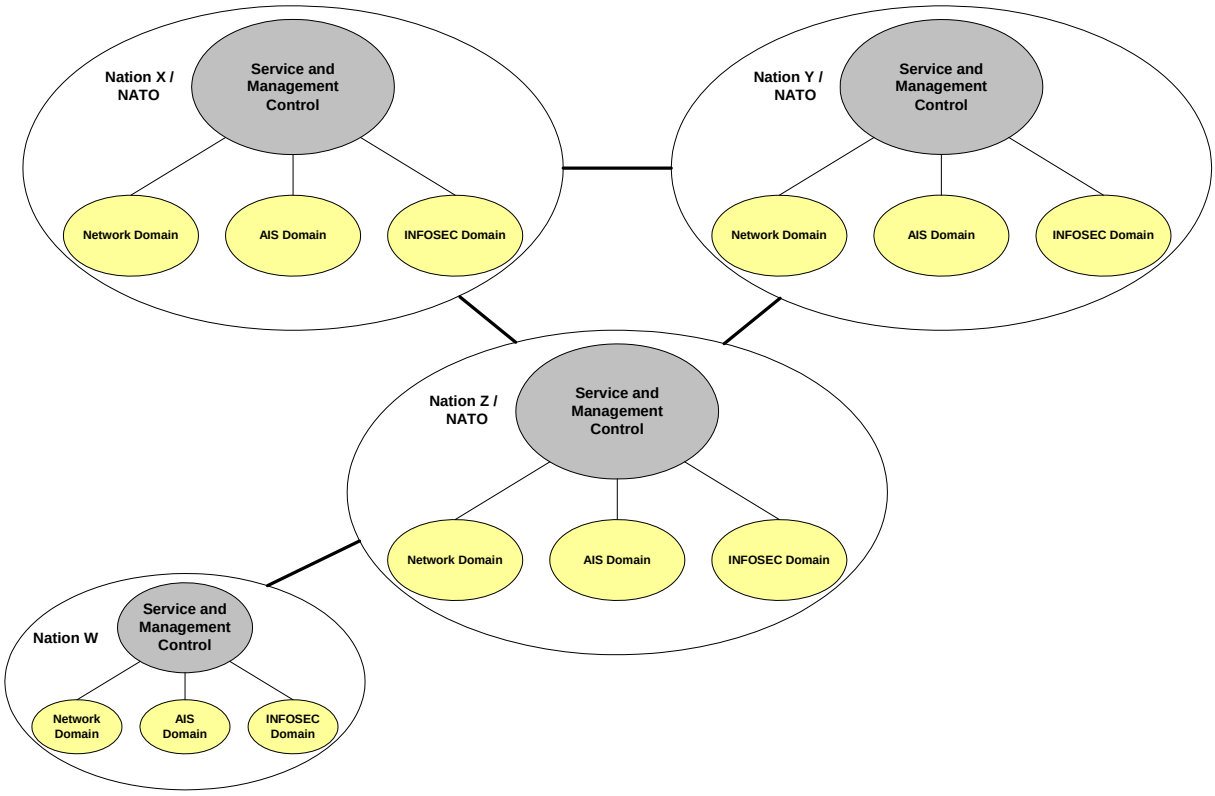


Figure 2 – NNEC FS - Generic coalition-wide service and management control

Service Level Agreements (SLA) plays a key role in the network centric process. This implies that, in the System Management of the Defense, the technological components and the available resources must be associated to SLA, whom the definition has to be harmonized at national level.

The aim is to move the management functions from the network level to the service level, this way integrating them in the end-to-end service chain and being represented as a SOA interface.

According to the NNEC FS recommendations, while keeping each organism its own operational autonomy, for the short term it is necessary to enhance the integration of management related to technologically homogeneous assets.

This suggestion is finalized to optimize the management resources in order to provide each manager of a global view of its assets and to manage end to end services in its own domain.

4.5 Evolution guidelines summary

The long term target to strike for the communication services is a fully integrated network in its own access and transport components, full-IP, wideband, able to grant end-to-end performances required by the user in terms of QoS and security in all its segments infrastructure, satellite, deployable and mobile (“black core network”).

From the “information & integration services” point of view, the long term target is the achievement of two “common environments”, for the classified domain and unclassified domain, both providing to the Units/TaskForces a complete set of information services.

On these basic “common environments”, common to the Armed Forces, will operate the Functional Area Services, i.e. applications specific to AA.FF/Jointed/NATO/Coalition and the “COI Services”, i.e. the information systems providing functions to groups or user communities.

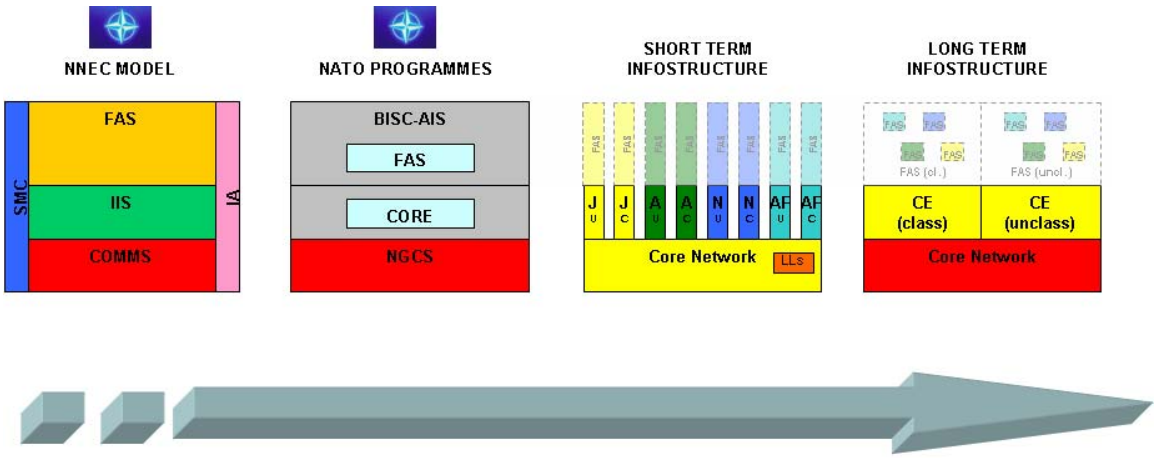
The management and control of systems is integrated with the aim of granting the SLAs agreed with the users, while security will have to be granted in an end-to-end way and it cannot alter performances provided by the network.

What described above has to be necessarily achieved by means of a step-by-step transformation process of the infrastructure which takes into account, in addition to the actual availability of the enabling technologies, also of the investments already done by military organizations in this field.

The long term target above described is shown in the following figure together with the evolution path of the Infostructure concept, starting from the indications of the NATO NEC FS and referring to the NATO programs of interest.

It is clear the correspondence between NII layers, the corresponding implementations in NATO and the Infostructure layers and the evolution in two steps of the Infostructure itself.

Figure 3 – Evolution of the Infostructure concept



J = Joint/Defence
A = Army
N = Navy
AF = Air Forces

LLs = Leased Lines

CE = Common Environment

In the following, the evolution guidelines described in this section will be "translated" into short-term targets and then in pragmatic update recommendations expressed by taking into consideration hypothetic needs and the known situation of assets.

5. INFOSTRUCTURE – SHORT TERM SCENARIOS

Scope of this section is to highlight the characteristics that networks and communication systems will have in order to complete a hypothetical first phase of the network centric migration process.

The short term scenario is deduced directly from the guidelines of the network centric infostructure (previous section).

The Infostructure model can be the one shown in the following figure:

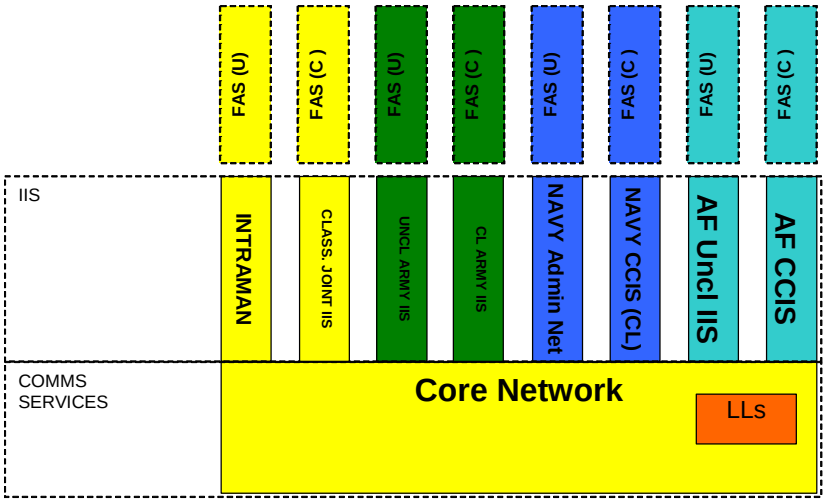


Figure 4 - Short term Infostructure concept

Both at communication services and information system levels, in the short term the trend is the interoperability achieved via federation of different assets, each one managed by the relevant owner.

The federation of systems, for the classified and unclassified domains, is achieved by standardizing implementation solutions and management procedures at information system and communication level.

The communication service layer is a federation of infrastructure, tactical and satellite, military and commercial, interoperable among them, able to grant the end-to-end transport of the IP flows according to the relevant security and QoS requirements.

The “core network” realizes the joint transport and includes, in addition to the assets owned by the Defense also the leased lines (LL).

As far as the management is concerned, today the transport network, which includes both access and backbone networks, is managed by one single entity, i.e. by a joint defense management center. Armed Forces IIS are already users connected to the edge of one single “core network”.

With reference to such a scenario, the following paragraphs identify the “macro-areas” which has to be considered strategic for the short-term transformation and for each one of them, describe the target to get.

5.1 Communication services

5.1.1 Infrastructure segment

5.1.1.1 Transport of traffic with QoS

The supply of “core services” implies the need of an IP network infrastructure able to support a number of typologies of information exchange.

In the short term, the migration towards IP of the Infrastructure Segment must necessarily be limited to the use of IP for native applications.

IP has not to be used as network protocol able to grant the QoS necessary to real-time and mission-critical traffic because IP, with relevant protocols and algorithms, as currently defined by the IETF, can only provide a statistic QoS and not deterministic and therefore not acceptable in a military network.

In the infrastructure case, only an increase of the amount of bandwidth coming from the expansion of the Core Network, together with the availability of well proven and consolidated technologies (ATM/SDH/MPLS), virtually makes the network resource able to grant the QoS.

On the other hand, in those networks (or network portions) based on bearers with limitations intrinsic to the physical mean (PDH radio relay, SATCOM), connection oriented protocols must be used such that support the dynamic bandwidth management and grant QoS. It is therefore envisaged to keep on the Core Network radio relay bearers the ATM layer already in operation, which is still considered the multiservice, connection-oriented protocol by definition.

5.1.1.2 Transport network

The transport infrastructure today is mainly based on radio relay backbone network and on the links realized by commercial operators (leased lines).

As far as the short term evolution of the transport component (Level 1 and 2 of ISO/OSI stack), the following evolution scenarios can be identified:

- **Consolidation of the national Defence backbone**
  The *desiderata* is to avail of an integrated transport infrastructure able to optimized the use of the network resources and to support all kind of communication services either sensible or untrusted. The consolidation of a common and integrated management policy will make easier to get the guarantee of end-to-end service, as requested by the information flows.

- **Increase of bandwidth to the user**
  The available bandwidth is a critical factor for the development of the information systems.

  In particular, the availability to all the users of collaboration services (e.g. audio/video teleconferencing systems), generally requiring a significant amount of bandwidth, will cause in the future a significant increase of traffic load on the network.

  In order to grant the required performances, the gradual rise of traffic must be followed by an optimization of the resources and an increase of the transmission capacity of the network and to increase the bandwidth to the

user means first of all optimization of the access networks and growth of the backbone capacity.

The optimization of the access networks mainly consists in the extension of fiber optic bearers and to use as back-up high capacity SDH microwave radio relays in order to realize redundant high reliability topologies.

The increase of transmission capacity can be achieved exploiting DWDM technology, able to provide some tens of Gb/s (in principle, with no need of replacing fibers, if any, in such a way to save the investments already done).

- **Coverage extension**
  The national coverage of the transport network must be such that all the user sites on the territory will be connected; this way minimizing the use of commercial leased lines.

5.1.1.3 Access to transport network

As far as the short term evolution of the access networks of the Defense, the following areas of interest can be identified:

- Use of IP protocol as standard switching layer;
- Optimization of the network assets;
- Extension of bandwidth to users;
- Centralization of the access points for both classified and unclassified traffic.

5.1.1.4 Optimization of user access

The user access sites must provide:

- standard equipment and routing protocols;
- standard mechanisms of access to the backbone network to increase reliability and manageability of the network traffic;
- diverse and classifiable in different categories on the basis of the amount of traffic they are able to manage.

The basic configuration of a typical access site shall have to include the following separated networks:

- Access to unclassified IP networks (e.g. Intranet);
- Access to nation classified IP networks (classified Intranet).

In addition, it has to be foreseen the availability of access to IP networks classified at NATO and international level.

The need in the same site of a number of different LANs physically separated comes from the lack, in the short term, of both multilevel security equipment able to operate the logical separation of information flows at different classification level or related to different domains, and of security standards that allow managing on the same LAN information flows at different classification level or related to different domains.

5.1.1.5 Non-IP networks

The proliferation of IP as convergence layer of communication services is not yet to be considered completed and, in the short term, legacy access networks using TDM technology (ISDN, EUROCOM, STANAG) will still be used.

To achieve the interoperability between legacy and IP users gateway elements will be used between TDM and VoIP users.

The gateway will perform the “adaptation” function between different technologies and will help activating the Voice over IP services:

This function can be embedded on plug-in units to be fitted into the switching equipment or on external modules/equipment, the latter referred in the NNEC FS as *Edge Proxies*, i.e. *devices acting as an interface to non IP networks and providing information proxy services as well as communications layer services*.

5.1.2 Satellite segment

As far as the short term evolution of the satellite segment, the following areas of interest can be identified:

- infrastructure applications
- deployable/mobile application

In the infrastructure environment, the satellite will have to be used for:

- backup of land links,
- link towards out-of-area deployable systems,
- connection of peripheral sites located in the country but not reached by the infrastructure network

In the deployable/mobile field, the satellite will be used:

- with a higher diversification of the operational bands to meet the increased OOA coverage need of the expeditionary operations (NNEC concept of resource pooling of SATCOM assets) and a wide variation of resources at short notice;
- for the connection of deployable systems one each other;
- for the connection of Deployable Command Posts or naval platforms towards mobile assets.

The satellite component must evolve in terms of geographic proliferation, quick deployability, “On the Move” operations and dynamic bandwidth management (with the use of IP protocol).

Therefore, it is envisaged the introduction of additional “Hub” sites in the national architecture both fixed and deployable, the latter ones also to be used in OOA, with the aim of decentralizing the “Anchor” function and improving “Failure Recovery” capabilities.

5.1.3 Deployable segment

5.1.3.1 Transport of traffic with QoS

In the short term, the migration towards IP of the deployable segment has to face the same challenges of the infrastructure segment, worsened by the peculiar characteristics like the poor availability of bandwidth which is due to the use of low capacity transmission systems, and like the poor link quality in terms of Bit Error Rate (BER).

Waiting for the consolidation of an IP technology able to meet such requirements, in the short term the IP flows will be transported on “virtual circuits” by means of connection-oriented protocols granting:

- QoS requested by the applications;
- Proper working over low capacity and high BER transmission channels,
- Quick convergence in case of changes of the network topology,
- Support of priority, pre-emption, security, user mobility.

Interventions will be mainly performed on the users’ area, where a gradual standardization of the voice and data interfaces towards Ethernet will be done.

5.1.3.2 Broadband wireless

Similarly to the infrastructure segment, for the deployable segment as well the distributed software applications distribute (typically the Command and Control systems) and the network information systems (core services) require a high transmission capacity.

The wide band in the connections among Command Posts in theater will be granted by fiber optic links in case of short distances deployments, or by means of wireless systems in operational conditions that cannot allow the use of fiber cables.

In this case, tactical radio will be used with traffic capacity at 34Mbit/s and broadband radio systems able to provide bandwidth of around ten Mbit/s over distances that can be assimilated to typical distances of a MAN (Metropolitan Area Network).

The broadband radio will allow high bitrate communication also among Command Posts and mobile users on vehicles.

5.1.4 Mobile segment

5.1.4.1 IP transport

The convergence over IP of communication services and the need to be as much sa possible stuck to the developments on the infrastructure and deployable side, practically impose the extension of IP to the mobile communication segment as well.

CNR networks and the communication devices of vehicular platforms and dismounted troops will have to be able to support at least “best effort” IP data traffic.

The migration to IP will allow integrating the mobile communications with those at Command Post level, already based on the same protocol.

5.1.4.2 Broadband Wireless

Mobile communications, from Command Post to the dismounted soldier in the operation theater, will be characterized by the use of links with capacity suitable to support the bandwidth-demanding Command and Control applications.

Vehicles will have to be equipped with broadband radio systems with characteristics suitable to the tactical environment such as redundancy, full meshed connectivity and integrated encryption capability.

In the future, such radio system will realize the main communication backbone for all the mobile assets of the Army and therefore this system should be installed at least on combat vehicles and on a subset of deployable systems as well, specifically those that need coordinating the mobile units on the battlefield (typically the Command Posts).

In addition, it shall be necessary to provide with these type of systems also the tactical units of other Armed Forces by keeping the full interoperability with the Army assets.

Short range communications (some hundreds of meters), usually inside a dismounted soldiers' squad and between soldier and vehicle, will be realized by means of wideband digital radios, handheld type (IPR – Individual Pocket Radio) and wireless LAN, with suitable solutions in terms of communication security and reliability. The Squad Commander, in addition to IPR and Wireless LAN, will have to be equipped with medium range communication system (some Km).

Currently, this latter need is met by legacy CNR VHF radios. While waiting for the maturity of technological solutions for medium range, wideband handhelds, in the short term it is necessary to identify a solution to enhance as much as possible the performances with the available systems.

5.2 Information & integration services

5.2.1 Common environment at infrastructure level

In the short term scenario, the implementation is foreseen of the first step of migration path towards the long term target represented by common basic services (the core services) from the strategic to tactical level, managed in a centralized way for the classified and unclassified domain.

The target in this phase is the federation of the information system currently available in the *intranets* of the Armed Forces with the aim of granting the full interoperability. The federation implies the standardization of the set of available information services and of the standards/protocols in use.

This approach involves in the same manner both the classified and unclassified domains.

With the aim of starting the transformation of a small community of users (easiest to manage) and in order to get a quick improvement in the joint forces integration of operational sites, the realization of the federation of network has to be planned on the classified domain first.

The concept is to create a complete collaboration environment in the joint Defense segment (a kind of ***joint secure intranet***) which increases the Defense C4I capabilities and among the Armed Forces services and, on the other side, which can represent a pilot project for the developments of other Armed Forces intranets, in the framework of achieving homogeneous solutions.

5.3 Information assurance

5.3.1 New generation IP encryption

The increase of the information systems available to users on the classified intranets and the consequent increase of the amount of exchanged information require the evolution of the IP encryption equipment.

To support the increase of bandwidth and to start the transition towards the IPv6 by keeping the interoperability with crypto currently in use, in the short term scenario new generation IP encryption equipment will have to be used able to:

- grant a throughput higher than 10 Mbps (current limit);
- support both IPv4 and IPv6 (IPv4/IPv6 dual stack).

5.3.2 Low rate voice and data secure communications

About low rate voice and data secure communications, in the short term it is necessary to improve the interoperability:

- among users belonging to different security domains (national, NATO, Coalition), currently separated;
- among users affiliated to heterogeneous networks (based on different technologies) without the introduction of gateways;
- among users equipped with devices supplied from various vendors, currently providing a poor interoperability.

5.3.3 KMI infrastructure

The need of automatically support the Information Assurance tasks in a intranet environment (joint or of an Armed Force) implies the need of realizing a national KMI including:

- a EKMS system for the automatic management of encryption keys.
- a PKI infrastructure for the creation and management of the certificates.

5.3.4 Security management system

This task is based on a collaborative approach for the IT security able to allow a more effective prevention and troubleshooting, intrusions and viruses.

5.4 System Management and Control

The NNEC vision of the communication networks mainly highlights the need of a higher level of coordination among management systems in order to allow an integrated management of the “end to end” services.

NNEC FS highlights the fact that nations/NATO will manage their networks autonomously but with a strong coordination between the coalition service management and control (SMCs).

The correlated aspects are shortly described in the following paragraphs.

5.4.1 Service Level Agreement – SLA

The Service Level Agreement (SLA) is a contract between user and management entity having as target a service performance.

The communication services provided by the network are ruled by SLAs.

The Service Level Agreements (SLAs) are seen in the NNEC view as the key ingredient of the future NII.

They are key to being able to provide information services, on an end to end basis, with adequate levels of performance, they are key to operating the NII as a FoS, and they are key to being able to prioritize and effectively utilize scarce system resources

A network with a management system able to provide a suitable support to the SLAs is able to set and update its own configuration depending on the requests generated by the users.

The compliance with the SLAs is granted by the network monitoring function which, in case of failure or inefficiency activates the proper redundancy mechanisms.

5.4.2 Core network – Joint system integration

In order to manage the SLAs stipulated with the users, the network management systems composing the “Core Network” must be able to operate in an integrated way.

In the short term, it is recommended to enhance the control of the network components by upgrading and putting into service the unified Control Centre of the Core Network-Joint for all the operational and technical management tasks. This Control Center will provide the overall view of the operational status of radio relay, fiber optic (as applicable), satellite transmission components and access components.

5.4.3 Integration of Deployable and Mobile systems

Each deployable or mobile asset must be controlled and managed from remote management system, at least for the critical parameters. Each tactical asset will be equipped with a Proxy function to interface the local equipment and interact with the higher management level with a common protocol.

This function will be realized by using the existing management elements where possible or by means of new devices with capabilities depending on the complexity of assets to be managed and therefore on the task to perform (alarm collection only, reduced configuration capabilities, full element management functions).

It will be then necessary to update the higher network management and network planning levels in order to develop management capabilities in line with the network centric migration, if not yet available.

5.5 Summary of the short term targets

The following table summarizes possible short term targets for the identified components of the Infostructure.

NII - components	Short term targets
INFRASTRUCTURE COMMUNICATION SERVICES	• Consolidation of the Core Network • Use of IP over ATM and SDH • Gateway between legacy and VoIP users
SATELLITE COMMUNICATION SERVICES	• Higher SATCOM capabilities on the home country • Dynamic management of the bandwidth • "On the Move" connectivity
DEPLOYABLE/MOBILE COMMUNICATION SERVICES	• IP Networking in the mobile segment • Wideband radio bearers
INFORMATION & INTEGRATION SERVICES	• Secure Common environment at infrastructure level for the jointed segment and federation of classified Armed Forces networks
INFORMATION ASSURANCE	• New generation IP encryption. • Secure communications over unsecured networks for voice and low rate data. • Automatic management of encryption keys and digital certificates
SYSTEM MANAGEMENT AND CONTROL	• Management of Service Level Agreements (SLA) • Remote control of Deployable and Mobile Assets

Table 1 – Short term targets

6. INFOSTRUCTURE EVOLUTION – PROCESS START

In the scenario described in the previous chapter, it is of the utmost importance to start an evolution process which allows achieving the short term objectives.

To this aim, the effort will have to be mostly focused on the implementation of the Core Network, by exploiting at best the most recent investments by means of a optimization and integration of the infrastructure, already in operation or being introduced.

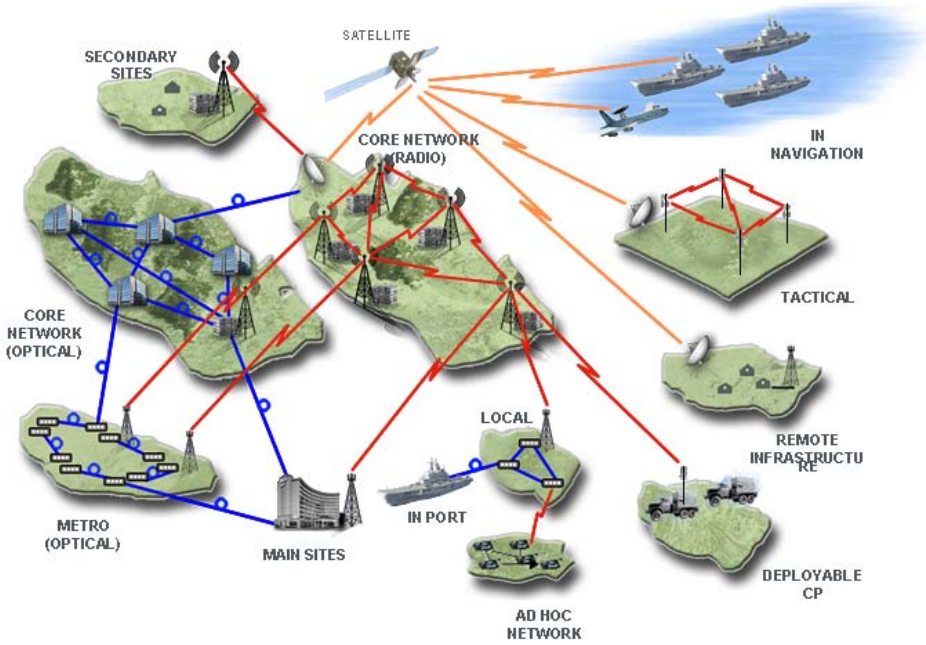
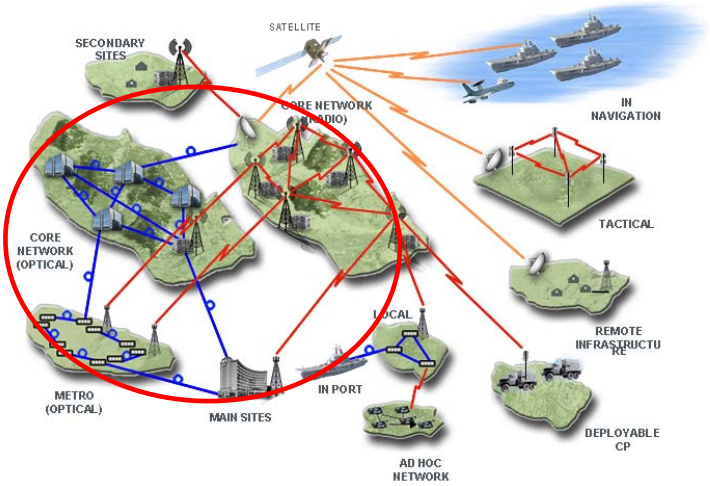


Figure 5 – Short-term –concept view

6.1 Communication Services - Infrastructure segment

In order to start the evolution process, a number of evolution tasks can be identified according to the scenarios defined above. These tasks are focused on the realization of the “Core Network”, by capitalizing the recent investments and via an optimization/integration of the infrastructure operational or available soon.



This section aims at recommending some possible interventions finalized to achieve a set of targets which contribute in reducing the criticalities today highlighted against the NCW migration process and to reach the maximum level of integration of all the network components, both strategic and tactical:

- Transport with QoS by means of ATM and SDH/DWDM technologies
- Interoperability between “Legacy” and IP users
- Consolidation and optimization of the network structure in terms of:
  - Completion/Enhancement of the radio relay network in both backbone and access layers
  - integration of the Networks in one single “Core Network”;
  - Design and implementation of high capacity fiber optic networks starting from MAN-type F.O. rings and consequent increase of traffic capacity on the backbone by using IP/ATM and SDH or DWDM technology (Gigabits).

6.1.1 Transport with QoS

The most viable solution for the transport with QoS in the short term is surely the use the ATM protocol on the radio relay backbone and the exploitation of consolidated technologies for high transmission capacity like SDH/DWDM on fiber optic rings.

6.1.2 Interoperability between “Legacy” and IP users

In the short term, it is foreseen the introduction of VoIP telephony and a progressive reduction of legacy subscribers (analogue, ISDN, EUROCOM).

In the coexistence phase, the interoperability among legacy and VoIP users will be achieved via “interoperability units” performing “Gateway” functions.

This interoperability must be granted both at basic call level (voice and data) and for the main user facilities. For instance, the transport of the PTT signal has to be supported for the communications towards single channel radios.

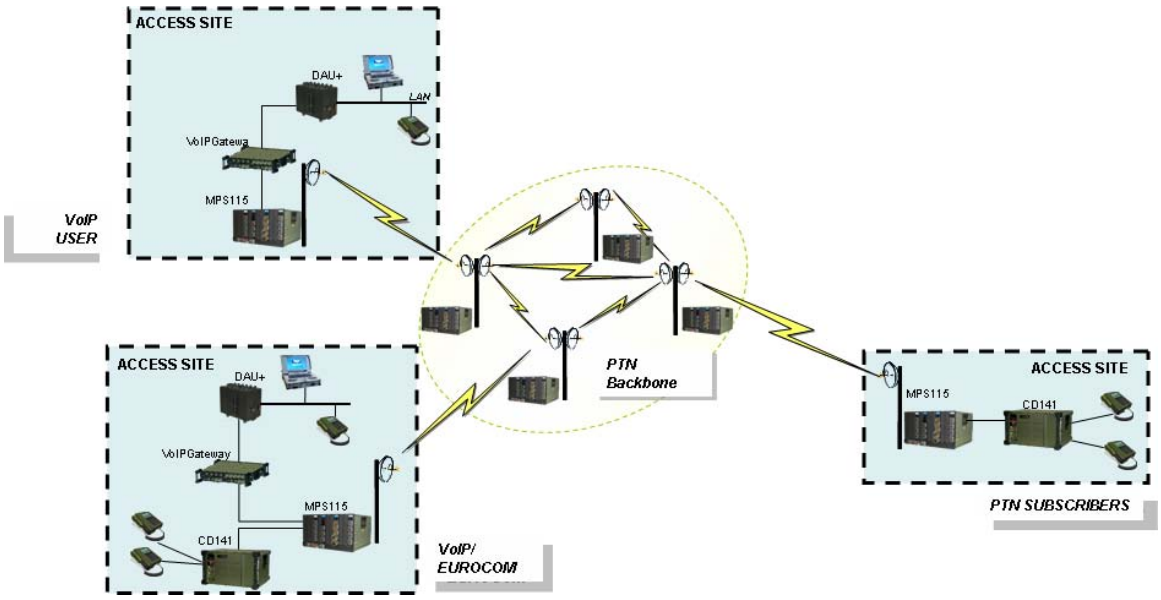


Figure 6 – Interoperability between “Legacy” and IP users

6.1.3 Optimization of the core network architecture

Standing the current architecture of the NDN radio relay transmission network, the first recommended activities can be summarized in the optimization of the access centers connectivity among them and to the backbone and in the increase of bandwidth to the user.

The concept of District Centers should be introduced and implemented, that is the main access nodes has to be identified and enhanced in order “to collect” all the aerial users belonging to the District. This collection can be performed by means of high capacity radio relays and/or fiber optic depending on the distribution of the users.

This intervention could allow removing current leased lines used to complete the network connectivity.

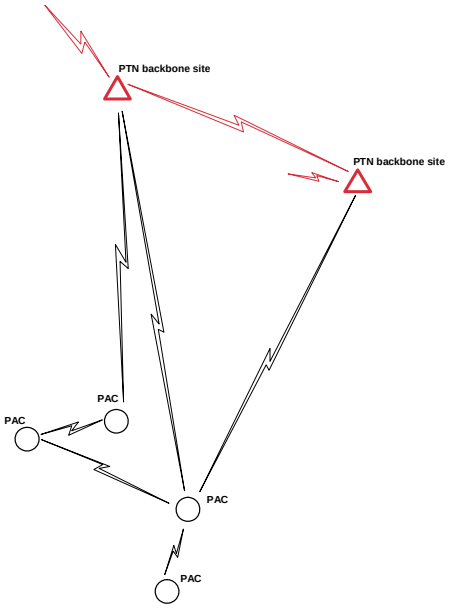
This approach could lead to achieve a new architecture of the infrastructure networks based on some regional Metropolitan Area Networks connecting the Primary Access Centers via microwave or fiber.

This way the national network will be composed by a number of regional/district networks.

These MANs will be connected to the high capacity backbone network of the Defense in F.O (towards the above mentioned transmission nodes SDH/DWDM in the district centers) and/or in microwave.

The following architecture schemes show an example of typical situation and an example of the described evolution.

After the intervention, the radio relay links currently operational could be removed or kept in operation (with increased capacity, if necessary) as backup



LEGENDA
PAC = Primary Access Site

Figure 7 – Current situation of the access links

The migration towards the structure previously described will have to make the access system homogeneous in all the most significant sites of the network.

The migration approach has to be based on the identification and classification of regional user sites according to the operational relevance (current and/or future) and of some importance from the point of view of the distribution of communications in the region.

Sites can be divided in the following categories:

- Primary Access Centers or District Centers (hereafter referred as DAC) – which roughly can correspond to sites like the Regional Management Centers
- Primary Access Centers (PAC) – which roughly may be assimilated to the regional sites with particular operational and/or architecture relevance:
  - Main Nodal Centers (ex. 1E);
  - Main Access Centers (ex. 1G1, 1X);
- Secondary Access Centers (SAC) – corresponding to Armed Forces units whom operational relevance is significant and their NCW service demand expected to increase.
- Minor Access Centers – corresponding to peripheral users with service demand increase not expected;
- Terminal Access Centers – users corresponding to minimum presence on the territory

Each type of access center will be standardized in terms of network and user interfaces.

The following scheme shows, as an example, the way the PAC and SAC connectivity could look like in the near future.

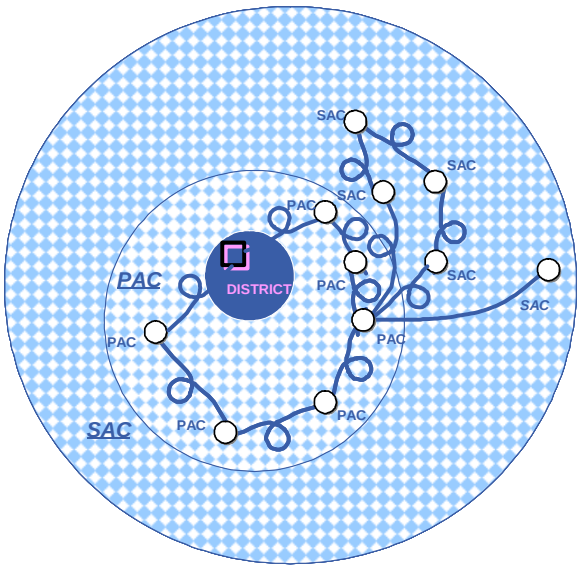
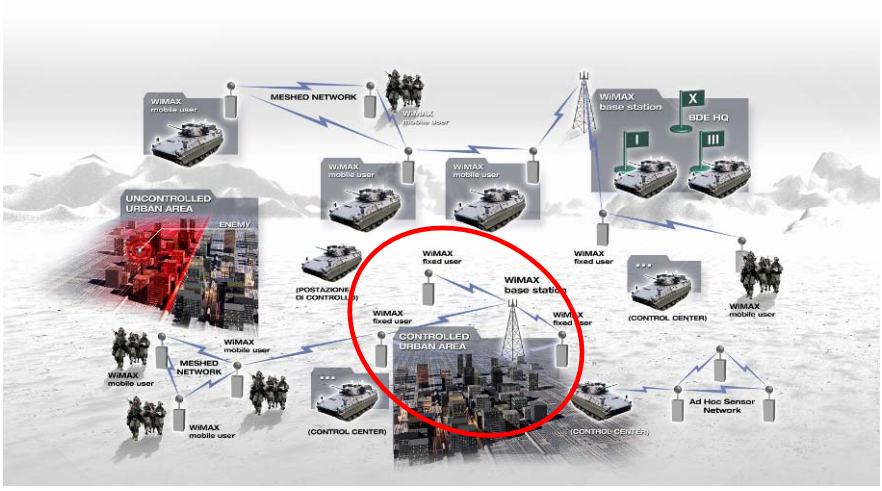


Figure 9 – Switching node PAC-SAC

6.1.3.1 Ad-Hoc Networks with WiMA in Controlled Areas

WiMAX is a broadband radio technology based on IEEE 802.16 standard.

This standard is purposely developed for wireless metropolitan area networks (MANs) and able to support fixed, nomadic and mobile access.



IEEE 802.16d (also 802.16-2004) copes with WiMAX fixed applications to:

- Implement a high-capacity PMP network (up to 70Mb/s over 20MHz)
- Connect fixed stations over different path lengths (up to 50km)
- Operate in LOS / NLOS conditions between base station and users
- Support IP technology
- Integrate security standards

WiMAX technology is suitable for NCW/NEC scenarios:

- Infrastructural - fixed connectivity for Military Units (see for instance the secondary or minor or terminal centers mentioned above), Airports, Ports, Arsenals
- Tactical - connectivity among CPs and Operational Units with MANET functionality
- Naval - connectivity among Naval Units and Coastal Infrastructure

For fixed applications in controlled areas, like in-country urban or rural areas, the intrinsic features of the WiMAX technology can be successfully employed for access networks when matched with full IP architectures.

Therefore, in order tu fully exploit the benefits introduced by this technology, a possible roadmap for fielding these systems has to be phased with the migration process towards full-IP.

Therefore, with reference to the sample architecture scheme shown, the following schemes shows the way legacy architectures of access networks based on PTP microwave links can be implemented by using WiMAX or can be migrated to PMP architecture with WiMAX.

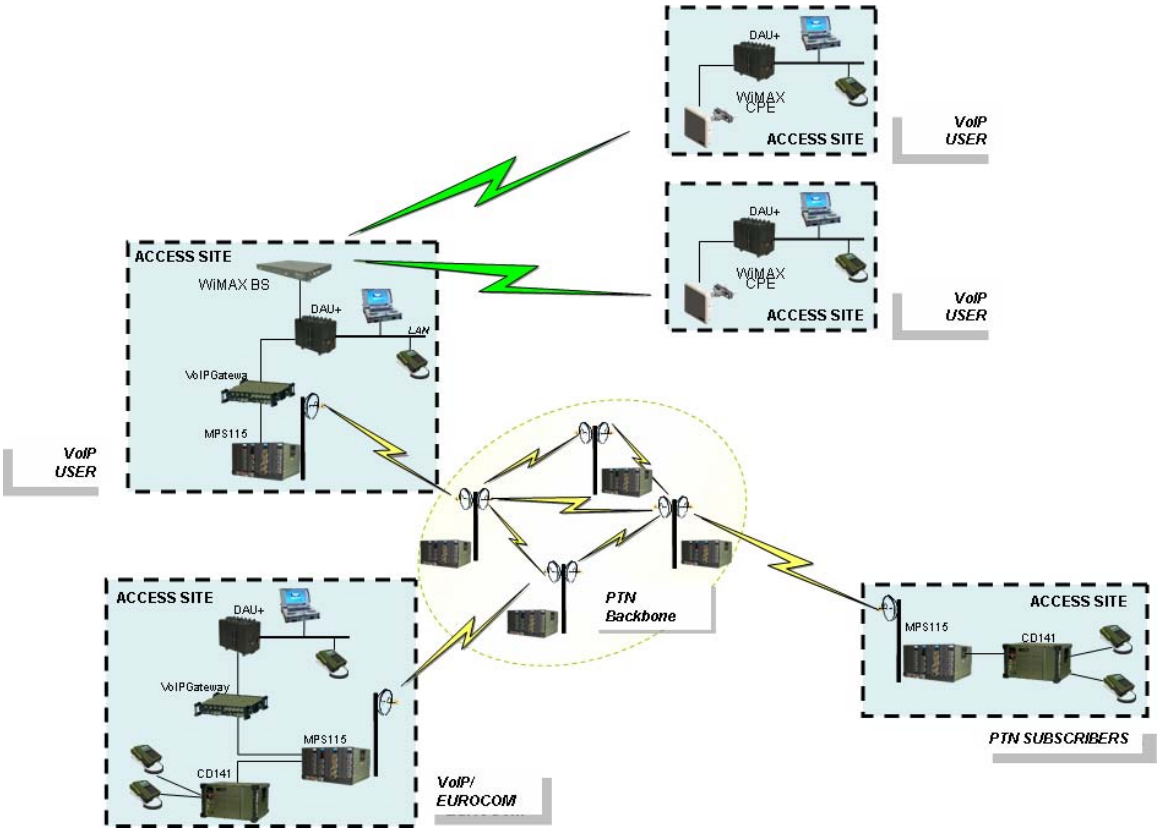
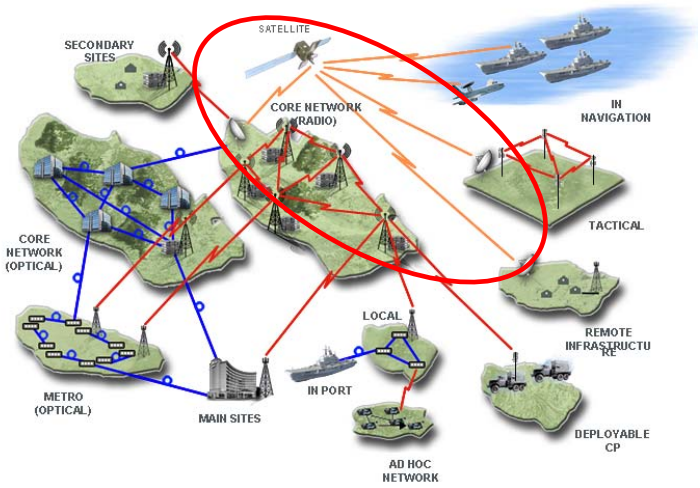


Figure 10 – Example of new sites with WiMAX connectivity

6.2 Communication Services -Satellite segment

"…NNEC will have to rely on a concept of resource pooling in which national military satcom and commercial satcom services are combined to meet the goals of coverage and sufficient capacity…"

"…The Coalition's operational and strategic networks must include the capability to securely connect to commercial teleports using commercial telecommunication services…"



As reminded in the NNEC FS, the SATCOM network properties (large bandwidth-delay product (BDP) links, time-varying channel, noise and dynamic network connectivity) impose avery strong organization effort in order to harmonize different communications technologies to achieve SATCOM networking, fully integrated with NATO and national network components.

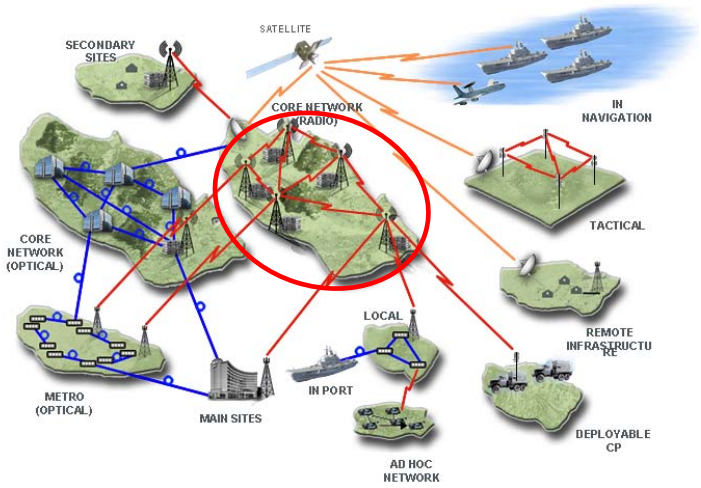
6.3 Communication Services - Deployable Segment

The following section summarizes the short terms interventions envisaged on the deployable assets.

6.3.1 Broadband Wireless

The most part of the tactical radio relays currently in use on deployable assets is operating in:

- NATO Band IV (capacity up to 8 Mb/s).
- NATO Band III+ (capacity up to 2 Mb/s)



The NATO Band IV tactical radios are mainly installed in the Transportable Sites with specific operational role as backup/enforcement of the strategic network.

The NATO Band III+ are mainly in use by other “Deployable” components such as the Gap Fillers. This equipment operates i.a.w. EUROCOM standard and are in full Indoor configuration.

Assets of new introduction in the short term should be provided with modern equipment with higher capacity (up to 8 or 34Mbit/s), still granting a minimum backward compatibility with existing radios and providing baseband interfaces compatible with the existing switching nodes.

It is also recommended that such equipment of new introduction also be fitted to operate the IP transport (with capacity even over the 34Mbit/s in Band IV).

This latter characteristic will play a key role in the migration towards the new scenarios based on full-IP.

6.3.2 IP transport

The recommended short term activities on the access components are finalized to a gradual migration of all the terminal access interfaces to the Ethernet standard.

Therefore all the analogue and EUROCOM digital terminals have to be replaced with VoIP telephones while serial data will be transported to Ethernet, as applicable.

This implies the need of introducing some kind of *access units* with layer 2 Ethernet switching capabilities and Ethernet uplinks towards the area network nodes where Ethernet access interfaces should be available.

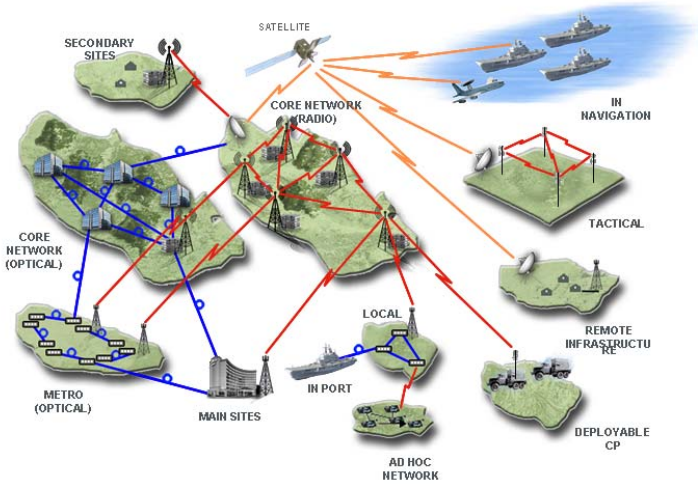
This uplink can be realized via cable, fiber or microwave point-to-point as well by using tactical radio relay with Ethernet interface.

It will be necessary to introduce a call processing unit for the VoIP users with Gateway capability in order to grant the interoperability with legacy.

6.4 Communication Services – Mobile segment

Main tactical assets interested by Digitalization process are:

- Deployable Command Posts (shelterised)
- Mobile Command Posts (vehicles)
- Combat and Troop Carrier vehicles,
- Blue Force Situation Awareness (BFSA)
- Battlefield Target Identification Devices (BTID),
- Soldier platforms.



The following picture shows the communication assets in the mobile segment already available or in the short term.

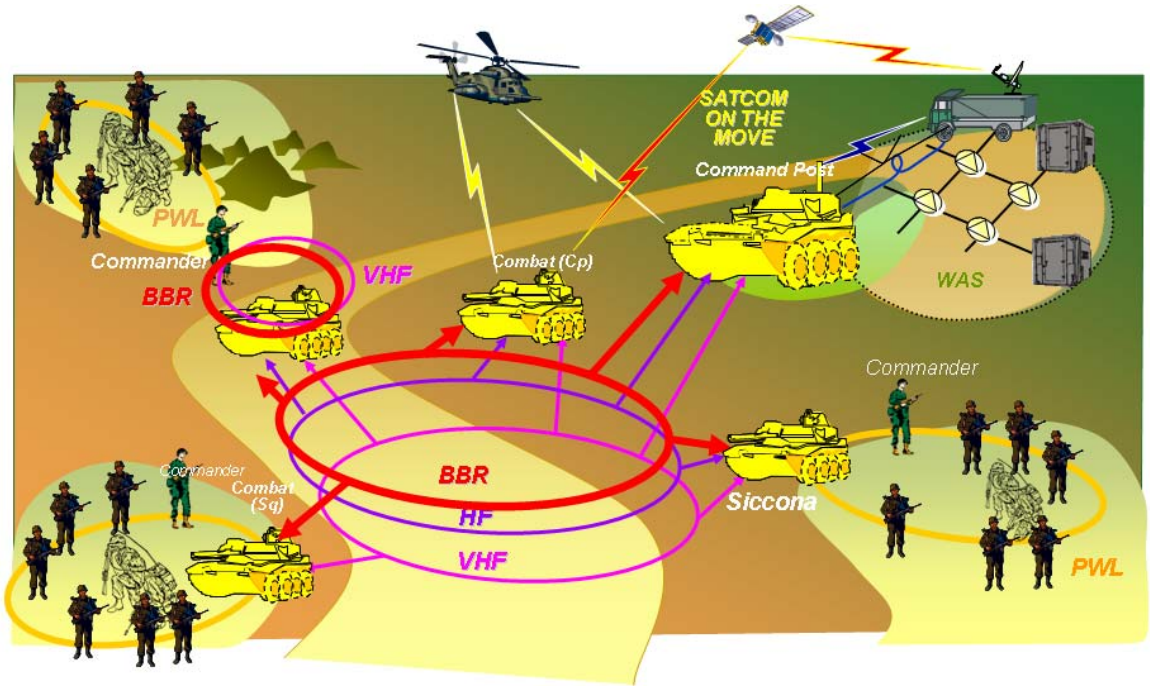


Figure 9 – Battlefield communications

6.5 Information Assurance

As preliminary remark to the envisaged short-term actions, it is necessary to highlight that the current security policies are not prepared to face and solve the new issues imposed by the NCW doctrine.

In particular, in the short term it is necessary to study at least the following points:

- Security algorithms and policies to be used in land tactical environment at low level, i.e. at Regiment-Soldier level, particularly in Coalition operations;
- One way connections from unclassified to classified networks in order to deliver basic information.

6.5.1 New generation IP Encryption

Taking into account the arising needs and the expected growth of bandwidth demand, it can be foreseen the introduction of IP encryption equipment able to support a throughput near to 100Mbit/s. The use of these devices is recommended in high bandwidth consuming network nodes. This could be the case of a secure intranet for joint use (classified core services).

6.5.2 KMI infrastructure

The KMI is composed by the PKI infrastructure and by the EKMS system described in the following.

6.5.2.1 PKI

In the short term, it is necessary the implementation of a PKI in order to build up a suitable support to the security management of classified intranets and federations of classified intranets. This PKI will have to be able to evolve to grant all the services such as digital signature, user authentication, equipment authentication, encryption related to COIs, generation of certificates for crypto equipment, etc).

6.5.2.2 EKMS system

The EKMS system for the automatic management of keys in the short term will have to be introduced and consolidated in order to activate an automatic key distribution in place of current manual procedures.

The distributed architecture with EKMS systems at A.F. distribution agency level has also to be evaluated.

This way doing, each Armed Force will be in contact with the National Distribution Agency and will receive automatically the encryption keys. Therefore, each A.F. distribution agency will operate as Central Distribution Facility (CDF) down to the crypto custodian(s).

The following scheme summarizes the KMI organization

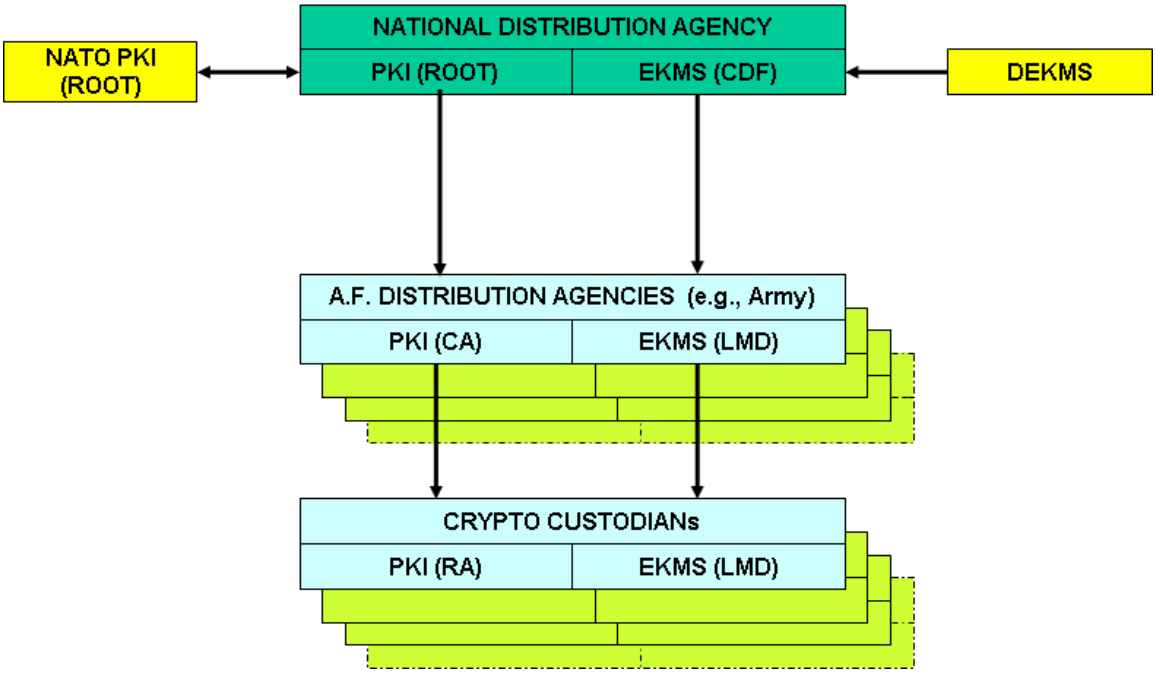


Figure 10 – KMI structure

The EKMS system will have the following main functionalities

- Support to estimate the keys needs
- Request of keys to Key Generation Centre
- Keys acquisition at the Central Distribution Facility (CDF)
- Key distribution to lower level (Local Distribution Facility LDF or final user)
- Key deletion (for expired and compromised keys)
- Electronic messaging
- Fault and anomalies management
- Accounting and auditing
- cryptographic functions performed only by the Key Processors
- Modular HW/SW architecture
- No limits to number of managed keys
- No limits to number of managed LDF
- Possibility to have redundant architecture

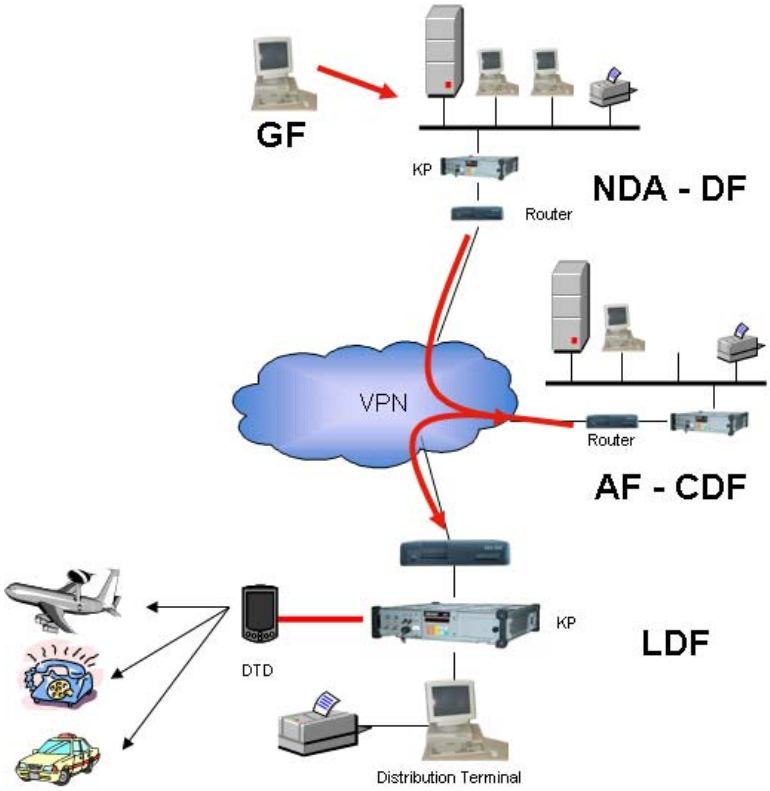


Figure 8 – EKMS system – concept architecture

6.6 System Management and Control

In order to optimize and integrate at Defense level the management systems, it is necessary to push for the progressive completion and enlargement of the areas of responsibility of the new network management system in order to reach the maximum extension of the managed assets and consequent dismission of old management systems.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	RTO-TR-IST-067 AC/323(IST-067)TP/317	ISBN 978-92-837-0111-8	UNCLASSIFIED/ UNLIMITED

5. Originator

Research and Technology Organisation
North Atlantic Treaty Organisation
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Technical Communications in Urban Operations

7. Presented at/Sponsored by

This Report documents the Findings of Task Group IST-067.

8. Author(s)/Editor(s)	9. Date
Multiple	September 2010
10. Author's/Editor's Address	**11. Pages**
Multiple	152

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other RTO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Cognitive radio
Dynamic spectrum allocation
Mobile Ad-hoc Networks (MANET)
Multiple-Input Multiple-Output (MIMO)
Procedures
Radio propagation
Software Defined Radio (SDR)
Tactical communications
Tactics, Techniques and Procedures (TTP)
Terrestrial Trunked Radio (TETRA)
Urban operations

14. Abstract

The purpose of the IST-067 research Task Group was to investigate and suggest ways to improve tactical wireless RF communications in a wide spectrum of urban operations. Increasingly, NATO nations are involved in traditional and non-traditional military operations in towns and cities occupied by a combination of non-combatants and hostile forces. Of all the missions faced by NATO, these combat and stability operations are the most challenging. Increasing dependence on information exchange at all levels is driving the demand for greater communication availability and throughput for military operations. Dependency on communications, especially at battalion level and below, is maximized in urban environments to compensate for loss of visual contact between small teams and to their parent organizations as they disappear into alleys, and multi-story buildings. While communications dependency is rising, its performance in urban settings suffers from radio frequency (RF) transmission range reductions caused by line-of-sight issues and attenuation due to buildings, structures and terrain; as well as interference from other local electromagnetic systems. Technology advances such as SDR, Cognitive Radio, MANET, MIMO, WiMAX, and Dynamic Spectrum Allocation have the potential to improve tactical communications in urban environments.

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

DIFFUSION DES PUBLICATIONS

RTO NON CLASSIFIEES

Les publications de l'AGARD et de la RTO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la RTO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents RTO ou AGARD doivent comporter la dénomination « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la RTO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (www.rto.nato.int) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National RTO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

CANADA
DSIGRD2 – Bibliothécaire des ressources du savoir
R et D pour la défense Canada
Ministère de la Défense nationale
305, rue Rideau, 9e étage
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5, 2750 Ballerup

ESPAGNE
SDG TECEN / DGAM
C/ Arturo Soria 289
Madrid 28033

ETATS-UNIS
NASA Center for AeroSpace Information (CASI)
7115 Standard Drive
Hanover, MD 21076-1320

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72, 92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
General Secretariat of Defence and National Armaments Directorate
5th Department – Technological Research
Via XX Settembre 123
00187 Roma

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
LOM PRAHA s. p.
o. z. VTÚLaPVO
Mladoboleslavská 944
PO Box 18
197 21 Praha 9

ROUMANIE
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353, Bucharest

ROYAUME-UNI
Dstl Knowledge and Information Services
Building 247
Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a informačné stredisko RTO
Demänová 393, Liptovský Mikuláš 6
031 06

SLOVENIE
Ministry of Defence
Central Registry for EU and NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar
Ankara

AGENCES DE VENTE

NASA Center for AeroSpace Information (CASI)
7115 Standard Drive
Hanover, MD 21076-1320
ETATS-UNIS

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa K1A 0S2, CANADA

Les demandes de documents RTO ou AGARD doivent comporter la dénomination « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications RTO et AGARD figurent dans les journaux suivants :

Scientific and Technical Aerospace Reports (STAR)
STAR peut être consulté en ligne au localisateur de ressources uniformes (URL) suivant: http://www.sti.nasa.gov/Pubs/star/Star.html
STAR est édité par CASI dans le cadre du programme NASA d'information scientifique et technique (STI)
STI Program Office, MS 157A
NASA Langley Research Center
Hampton, Virginia 23681-0001
ETATS-UNIS

Government Reports Announcements & Index (GRA&I)
publié par le National Technical Information Service
Springfield
Virginia 2216
ETATS-UNIS
(accessible également en mode interactif dans la base de données bibliographiques en ligne du NTIS, et sur CD-ROM)

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

BP 25

F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

DISTRIBUTION OF UNCLASSIFIED RTO PUBLICATIONS

AGARD & RTO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all RTO reports, or just those relating to one or more specific RTO Panels, they may be willing to include you (or your Organisation) in their distribution.

RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for RTO or AGARD documents should include the word 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of RTO reports as they are published, please visit our website (www.rto.nato.int) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National RTO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

CANADA
DRDKIM2 – Knowledge Resources Librarian
Defence R&D Canada
Department of National Defence
305 Rideau Street, 9th Floor
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
LOM PRAHA s. p.
o. z. VTÚLaPVO
Mladoboleslavská 944
PO Box 18
197 21 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72, 92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate
Research Directorate, Fakinos Base Camp
S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
General Secretariat of Defence and
National Armaments Directorate
5th Department – Technological
Research
Via XX Settembre 123
00187 Roma

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6, 061353, Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko RTO
Demänová 393, Liptovský Mikuláš 6
031 06

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
SDG TECEN / DGAM
C/ Arturo Soria 289
Madrid 28033

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Knowledge and Information
Services
Building 247
Porton Down
Salisbury SP4 0JQ

UNITED STATES
NASA Center for AeroSpace
Information (CASI)
7115 Standard Drive
Hanover, MD 21076-1320

SALES AGENCIES

NASA Center for AeroSpace Information (CASI)
7115 Standard Drive
Hanover, MD 21076-1320
UNITED STATES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa K1A 0S2, CANADA

Requests for RTO or AGARD documents should include the word 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of RTO and AGARD publications are given in the following journals:

Scientific and Technical Aerospace Reports (STAR)
STAR is available on-line at the following uniform resource locator: http://www.sti.nasa.gov/Pubs/star/Star.html
STAR is published by CASI for the NASA Scientific and Technical Information (STI) Program
STI Program Office, MS 157A
NASA Langley Research Center
Hampton, Virginia 23681-0001
UNITED STATES

Government Reports Announcements & Index (GRA&I)
published by the National Technical Information Service
Springfield
Virginia 2216
UNITED STATES
(also available online in the NTIS Bibliographic Database or on CD-ROM)

ISBN 978-92-837-0111-8